# ACADEMIC GRADUATION MONITORING REPORT

2023

European Association for Biometrics (EAB)

version: 2024-09-20

Email: secretariat@eab.org

# RESEARCH MONITOR CONTENT

# PREFACE

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

# MONITOR
# PHD-THESES

## WERONIKA GUTFETER - MULTI-VIEW NEURAL NETWORKS FOR FACIAL IDENTIFICATION

**Full Title:** Multi-view neural networks for facial identification
**Institution:** Warsaw University of Technology
**Supervisor:** Andrzej Pacut
**Contact email:** weronika.gutfeter@nask.pl

**Abstract:**
The main goal of the thesis is to solve the problem of face identification in multi-view face images. Datasets that consist of multi-view face images can be obtained in various scenarios. One of the typical uses is police booking photography, where the specialists are obligated to acquire a set of face images from strictly defined angles for each suspect. Another scenario is also one of the methods employed in 3D face recognition. As the 3D models are quite heavy and computationally demanding, a typical solution to that problem is to transform 3D data into a set of 2D images showing the object from different views. This approach can be named as multi-view object classification. After preliminary experiments, we observed that most of the state-of-the-art algorithms are optimized to recognize frontal images and there is a significant drop in accuracy when identification is made on sets containing extreme views like full profile pictures. In our work, we conducted a survey of methods that can be used for creating biometric templates from image collections with non-frontal faces. We analyzed various approaches like 3D face alignment, single-view template aggregation and multi-view networks. For our experiments, we adapt methods that have been proposed for multi-view object recognition, namely MVCNN and RotationNet. However, we should emphasize that there exists a difference between these two domains. Multi-view object recognition is typically based on a closed dictionary of labels and objects are represented by a relatively large number of views while faces are organized in the sets of three or five probes and the possibility of new identifier registration is crucial for the system. For the purpose of the experiments, it was necessary to collect face data that is structured in the following manner and to define adequate testing scenarios. We also introduce a new multi-view model in which we apply multi-head attention for data flow aggregation. We named it SygnaT. SygnaT solves some of the limitations of the previous models, as it does not require a strict number of probes or a specific order in the view set. All of the proposed multi-view networks gain higher results than the single-view approaches. For the SygnaT network, the Rank-1 accuracy is higher by 6% in a full identification test and by 18% in a test on profile pictures. Each of the analyzed solutions was built using deep convolutional networks and there is a common backbone for all of them. The backbone is implemented with ResNet-50 architecture. Therefore weights can be transferred from the baseline single-view model which was trained on VGGFace2 to make all the models more unified and easily comparable. We showed that the multi-view networks work in various face identification scenarios, we tested all solutions in closed and open-set tests. Moreover, we conducted an experiment with SygnaT on an unstructured dataset (face recognition benchmark IJB-C) and proved that also this configuration is better than the single-view model approach.

## MARTIN PERNUŠ - FACE IMAGE EDITING

**Full Title:** Automatic image editing with generative neural network models based on linguistic descriptions
**Institution:** University of Ljubljana, Slovenia
**Supervisor:** Simon Dobrišek
**URL:** https://repozitorij.uni-lj.si/Dokument.php?id=178397&lang=slv
**Link description:** The PDF is available for the thesis - in Slovene
**Contact email:** vitomir.struc@fe.uni-lj.si

**Abstract:**
In recent years, the fields of computer vision and artificial intelligence have made great strides in the field of image generation using deep-learning methods. Behind these results are generative deep neural network models that are capable of generating photorealistic and visually convincing images of different objects and even complex scenes. Despite advances in image generation, the understanding of generative models and their application to image editing is still limited. Here, we use the term "understanding" to denote the ability of robust learning of generative models and the link between latent and target (image) probability distributions of the data. There is not yet an automated management mechanism over general image editing that would allow editing only specific image properties. Systems that would allow image editing with generative models based on linguistic descriptions would contribute significantly to applications in various fields such as autonomous driving, robotics, manufacturing, design, entertainment, animation, and others. In such systems, the user could influence the appearance and semantic content of an image by means of a textual or speech description of the visual scene. The main topic of the PhD thesis is building a generative neural network system in combination with linguistic description, where the goal is to extract information about desired features or changes of images from linguistic descriptions and then use this information for image editing. The starting point for our research is a generative neural network, which is built in a way that enables creating or editing a desired image given linguistic or more structured information. We present several different original contributions as part of our PhD thesis. The first original contribution is a new method for editing facial attributes called MaskFaceGAN. Given a generative image model, the presented method allows the manipulation of different facial features (e.g. hair colour, eyebrow type, nose size). The target linguistic information required for face editing is given in the form of the selection and intensity of a particular facial feature. By designing a special generative network inverting process, the proposed solution enables high-resolution face editing, which also allows simultaneous editing of multiple features and resizing of individual facial parts. Experiments and a user study are performed on different datasets, which show the advantages of the proposed MaskFaceGAN method over competing technologies. The next original contribution is the ChildNet method, a model that is able to predict the appearance of children given the images of their parents. ChildNet is able to synthesize an image of a child given an input image of the parents, where additional linguistic information can be added to the model in the form of additional requirements on the child's appearance (age and gender). We also present a new high-resolution dataset that is designed to learn models for image synthesis given sibling relationships. We evaluate ChildNet against other competing technologies, where our method is shown to more accurately estimate the appearance of the child, producing images of high quality and resolution. The last original paper presents the FICE method, which addresses text-based fashion image editing. The linguistic information here is given in its most raw form, i.e. in the form of text. The method is capable of processing textual descriptions that can express a wide vocabulary. The concept of image editing is based on the inversion of a generative network, where the model itself is specialised for editing fashion images. To evaluate the quality of the method, we propose several different metrics focusing on image quality, person pose preservation, semantic relevance and identity preservation. We compare the methods with other text-based image editing technologies, where the FICE method is shown to outperform in all tested metrics. In summary, all the original contributions focus on understanding and building generative models or developing systems where the target linguistic information is fed in some way into our model to generate the desired image. The results of the research demonstrate the potential of generative models for image editing and the importance of understanding the link between latent and target probability distributions. The proposed methods and systems have the potential to contribute significantly to a wide range of applications in various fields.

## PARIZA REZAEE BORJ - ONLINE GROOMING DETECTION ON SOCIAL MEDIA PLATFORMS

**Full Title:** Online Grooming Detection on Social Media Platforms
**Institution:** NTNU
**Supervisor:** Patrick Bours
**URL:** https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/3061201
**Contact email:** patrick.bours@ntnu.no

**Abstract:**
Online grooming detection has become a critical research topic in the era of extensive data analysis. It is essential to protect vulnerable users, particularly adolescents, against sexual predation on online platforms and media. However, many factors challenge online grooming detection, which leads to a high-risk problem for youth. The primary goal of this research work is to provide techniques that increase children's security on online chat platforms. To this extent, many experiments have been conducted to create models fulfilling our research goal. As such, this thesis contains a comprehensive survey of child exploitation in chat logs that provides the readers with a deep knowledge of the problem, possible research gaps, and proposed solutions. In this research, we split the online grooming detection problem into several subproblems, including author profiling, predatory conversation detection, predatory identification, and data limitations issues. The leading theory behind the author profiling in this problem comes from the fact that online predators provide fake identities to tarp their young victims. At the same time, children's characteristics differ from the ones who imitate a minor, which leads us to detect the gender of users in this research. In this thesis, we propose a gender detection model that can recognize the gender of authors based on their keystroke dynamics features. This research also provides a fake identity detection technique with a high performance that detects users who are dishonest about their identity. Providing an automatic predatory conversation detection system facilitates law enforcement authorities to act on time before any tragedy occurs. Therefore, we have examined and proposed several predatory conversation detection and predatory identification techniques focusing on finding the best feature vectors and embeddings that lead to the best performance in online grooming detection. This thesis also aims to gain deep knowledge about predatory behaviour with semantic analysis. We might lose some semantic information by applying conventional embeddings such as Word2vec or GloVe feature vectors since they provide a single word embedding for a term in different contexts. At the same time, humans show their motivations in phrases or sentences rather than single terms. So, we provide an online grooming detection model based on extracting embeddings from sentences rather than single words. We apply contextual model based such as Bert-based and RoBerta-based systems for each sentence. Several constraints, such as privacy and security issues, availability, and the imbalanced nature of the datasets, challenge online grooming datasets. The number of predatory chat logs is considerably lower than the other online conversations, leading to a highly imbalanced data problem. It is challenging to build a machine learning model based on imbalanced datasets, which motivates us to provide a model to handle this issue. This research proposes a model that uses a hybrid sampling and class re-distribution to gain augmented data for coping with highly imbalanced datasets. We also improve the diversity of classifiers and feature vectors by perturbing the data along with the augmentation in an iterative manner. Finally, we conclude our research by discussing potential research gaps and open problems and proposing possible solutions for them to give deep insights to the readers of future work based on the work of this thesis.

## HEMLATA TAK - END-TO-END MODELING FOR SPEECH SPOOFING AND DEEPFAKE DETECTION

**Full Title:** End-to-End Modeling for Speech Spoofing and Deepfake Detection
**Institution:** EURECOM
**Supervisor:** Nicholas Evans and Massimiliano Todicso
**URL:** https://www.eurecom.fr/publication/7273
**Contact email:** evans@eurecom.fr

**Abstract:**
Voice biometric systems are being used more and more in various applications, including banking, call-centres, airports, access control, and forensics. These systems use automatic speaker verification technology for secure user authentication, but are susceptible to spoofing attacks, also known as presentation attacks. Spoofing is now a growing concern in academia and industry. It is essential to mitigate the threat, especially in high security scenarios. Recent advances in artificial intelligence have greatly improved the capability of generating synthetic voices, making it even more challenging to distinguish between genuine and fake audio. There is hence a need for more robust, and efficient detection techniques. This thesis proposes novel detection algorithms which are designed to perform reliably in the face of the highest quality attacks. The first contribution is a non-linear ensemble of sub-band classifiers each of which uses a classical Gaussian mixture model (GMM). Competitive results with such a traditional approach show that models which learn sub-band specific discriminative information can substantially outperform models trained on full-band signals. Given that deep neural networks are more powerful than GMMs and can perform both feature extraction and classification, the second contribution of this thesis is a RawNet2 model. It is an end-to-end approach to anti-spoofing and deepfake detection which automatically learns discriminative features directly from raw waveform inputs. Results show that RawNet2 performs reliably even in the face of previously unseen spoofing attacks. End-to-end modelling can be seen as a joint feature extraction and classification framework which streamlines the processes of training and evaluation. The third contribution of this thesis includes the first use of graph neural networks (GNNs) with an attention mechanism to model the complex relationship between discriminative information present in spectral and temporal domains. We propose an end-to-end spectro-temporal graph attention network called RawGAT-ST. Like the RawNet2 model, it also operates directly upon raw waveform inputs. An attentive graph pooling layer is incorporated to identify and retain informative nodes and to discard irrelevant ones, thereby reducing computation and also improving discrimination power. The RawGAT-ST model is further extended to an integrated spectro-temporal graph attention network, named AASIST which exploits the relationship between heterogeneous spectral and temporal graphs. The use of a heterogeneous graph attention network allows for the integration of different types of nodes/edges which contain different feature characteristics. GNN-based countermeasures leverage the inherent information in both domains concurrently, improving the detection of more sophisticated spoofing attacks, while also improving upon generalisation. The final contributions relate to the development of a novel data augmentation technique and a self-supervised front-end which improves generalisation and domain-robustness under more practical conditions. Acquiring training data that is representative of spoofing attacks with near-boundless variability is impractical or even impossible. Nonetheless, the performance of spoofing countermeasures relies on the use of sufficiently representative training data. To address this issue, we propose a raw data augmentation technique called RawBoost. RawBoost improves spoofing detection reliability in the face of nuisance variation stemming from unknown encoding, and transmission conditions and from different microphones and amplifiers, and both linear and non-linear device-generated distortion, all of which characterise a logical access or telephony scenario. An alternative approach is to use a front-end in the form of readily available self-supervised, pre-trained speech models trained on large databases. The combination of a self-supervised front-end with RawBoost brings substantial improvements in performance for the ASVspoof 2021 logical access and deepfake databases. The work reported in this thesis has redefined the state-of-the-art in anti-spoofing, with results for RawGAT-ST, AASIST and SSL-based countermeasure solutions all being the best reported at the time of publication, and with those for the self-supervised based countermeasure remaining the best reported to date.

## MONA HEIDARI - RECOGNITION OF DISEASED FINGERPRINTS

**Full Title:** Connection of algorithms for removal of influence of skin diseases on the process for fingerprint recognition
**Institution:** Brno University of Technology
**Supervisor:** Prof. Ing. Martin Drahanský, Ph.D.
**URL:** https://drive.google.com/file/d/1dxsrDM0QnuQPq7YU-oJ8Ieqf-ldgNTxh/view?usp=sharing_eil_m&ts=6509711b
**Link description:** Before the defence the link is unofficial, afterwards the link to the faculty webpage will be provided
**Contact email:** martin@drahansky.cz

**Abstract:**
This thesis focuses on data structures, image processing, and computer vision methods for detecting and recognizing diseases in fingerprint images. The number of developed biometric systems and even used biometric characteristics is increasing. It is widely accepted that an individual's fingerprint is unique and remains relatively unchanged throughout life. However, the structure of these ridges can be changed and damaged by skin diseases. As these systems depend heavily on the structure of an individual's fingertip ridge pattern that positively determines their identity, people suffering from skin diseases might be discriminated against as their ridge patterns may be impaired. Likely, fingerprint devices have not been designed to deal with damaged fingerprints; therefore, after scanning the fingerprint, they usually reject it. The influence of skin disease is an important but often neglected factor in biometric fingerprint systems. An individual might be prevented from using specific biometric systems when suffering from a skin disease that affects the fingertips. Collecting a database of fingerprints influenced by skin diseases is a challenging task. It is expensive and time-consuming, but it also requires the assistance of medical experts and the ability to find willing participants suffering from various skin conditions on fingertips. The raw diseased fingerprint database is first analyzed to provide a solid foundation for future research. Common signs among all fingerprint images affected by the disease are found for every particular disease, and a general description of each disease and its influences is defined. Then we automatically assign the label based on a combination of the known state of the fingerprint image. The proposed solution is integrated with different algorithms focused on image processing libraries and computer vision methods for object detection. The solution has been evaluated on damaged fingerprint datasets and highlights the state of the art implementations using proposed techniques. The state of the art technique for disease detection implementations uses texture analysis and feature detection by comparing the intensity values of pixels in a small neighborhood in an image. Due to the complexity of each disease pattern, the combination of texture analysis algorithms leads to better detection results. The combination of Gray Level Co-occurrence Matrix (GLCM), Local Binary Pattern (LBP), orientation field, and mathematical morphology can detect damage (artifacts) in fingerprint images. Combining these features makes it possible to identify changes in the texture and shape of the fingerprint flow caused by diseases. These techniques capture different aspects of the texture and shape of the damage in fingerprint images and lead to identifying changes in the texture caused by diseases. In the stages of the detection process, mathematical morphology operations are applied to improve the structural details by removing small irregularities in the image and simplify the shape of objects, making it easier to identify and isolate them expanding the boundaries of objects in an image or filling gaps and connect broken parts of objects, leading to better object detection and recognition. At the end of the detection process, coherence is applied to show the quality evaluation of fingerprint image patches into three types healthy, damaged, and background. Overall, the proposed solution showcases the effectiveness of integrating multiple image processing and computer vision algorithms for disease detection in fingerprint images. The combination of these algorithms can accurately detect and localize disease patterns in damaged fingerprint datasets, thus providing a reliable solution for disease detection in forensic applications.

## ROBERTO CASULA - THE ART OF FINGERPRINT SPOOFING

**Full Title:** The Art of Fingerprint Spoofing
**Institution:** University of Cagliari
**Supervisor:** Gian Luca Marcialis
**Contact email:** casula.roberto103@hotmail.it

**Abstract:**
The natural instinct of every human being is to want to protect themselves from their surroundings. Starting from the classic passwords required to access specific information, we moved on to safer and more accurate methods based on the specific characteristics of each user: biometrics. The first identification using fingerprints, in fact, dates back to the last years of the 1800s and was used by the police station for the criminal identification. From that moment on, the various biometric authentication systems based on fingerprints began to spread and, consequently, the first bad guys began to create false fingerprints to access the systems themselves. Fingerprint spoofing techniques became effective against biometric sensors thus leading to the creation of Liveness Detector modules, capable of detecting the liveness of a fingerprint: from handcrafted methods to deep neural networks, the performances, tested on datasets of first editions of the LivDet competitions containing live prints and fake prints created with the consensual method, show high security. And no matter how much a "prey" may commit to defending itself, there will always be a "predator" ready to improve itself to reach its end. In this PhD thesis a new fingerprint falsification technique will be presented, able to show the vulnerabilities of the detectors presented in the last two editions of the International Fingerprint Liveness Detection Competition. This method based on latent fingerprints will be analyzed primarily from a pseudo-consensual point of view, to then move on to a completely non-consensual case study, simulating a real attack on a specific user. An adversarial perturbation technique via GAN will then be presented, in order to create, first digitally and then physically, a print that alters the result of the classification from fake to live. For this type of process the cross-sensor explainability will be studied, evaluating the performances step by step with the best detectors of the latest LivDet competitions.

## MARCO MICHELETTO - FUSION OF PRESENTATION ATTACKS DETECTION AND MATCHING

**Full Title:** Fusion of fingerprint presentation attacks detection and matching: a real approach from the LivDet perspective
**Institution:** University of Cagliari
**Supervisor:** Gian Luca Marcialis
**URL:** https://iris.unica.it/handle/11584/357306
**Link description:** Ph.D. thesis description
**Contact email:** marco.micheletto@unica.it

**Abstract:**
The liveness detection ability is explicitly required for current personal verification systems in many security applications. As a matter of fact, the project of any biometric verification system cannot ignore the vulnerability to spoofing or presentation attacks (PAs), which must be addressed by effective countermeasures from the beginning of the design process. However, despite significant improvements, especially by adopting deep learning approaches to fingerprint Presentation Attack Detectors (PADs), current research did not state much about their effectiveness when embedded in fingerprint verification systems. We believe that the lack of works is explained by the lack of instruments to investigate the problem, that is, modeling the cause-effect relationships when two systems (spoof detection and matching) with non-zero error rates are integrated. To solve this lack of investigations in the literature, we present in this PhD thesis a novel performance simulation model based on the probabilistic relationships between the Receiver Operating Characteristics (ROC) of the two systems when implemented sequentially. As a matter of fact, this is the most straightforward, flexible, and widespread approach. We carry out simulations on the PAD algorithms' ROCs submitted to the editions of LivDet 2017-2019, the NIST Bozorth3, and the top-level VeriFinger 12.0 matchers. With the help of this simulator, the overall system performance can be predicted before actual implementation, thus simplifying the process of setting the best trade-off among error rates. In the second part of this thesis, we exploit this model to define a practical evaluation criterion to assess whether operational points of the PAD exist that do not alter the expected or previous performance given by the verification system alone. Experimental simulations coupled with the theoretical expectations confirm that this trade-off allows a complete view of the sequential embedding potentials worthy of being extended to other integration approaches.

## TOMÁŠ GOLDMANN - FACE RECOGNITION USING NEURAL NETWORKS AND ACCELERATORS

**Full Title:** Research in the field of biometric detection and recognition of individuals using facial image data
**Institution:** Brno University of Technology
**Supervisor:** Prof. Ing. Martin Drahanský, Ph.D.
**Contact email:** martin@drahansky.cz

**Abstract:**
Biometric recognition has long since become a common concern in various fields of study, including forensics, anthropometry, biometrics, and computer science. This thesis focuses on the development of an approach to create datasets for the evaluation of face recognition algorithms, with an emphasis on the preservation of facial features. Such datasets open up new possibilities for the evaluation of face recognition algorithms, which were previously hindered by the limited sample size of the datasets usually used. Through extensive research in the field of face recognition algorithms and modern neural network techniques, algorithms for face detection and recognition on embedded devices have been developed. These algorithms are based on the EfficientNet feature extractor.

## BLAŽ MEDEN - FACE DEIDENTIFICATION WITH GENERATIVE NEURAL NETWORKS

**Full Title:** Face deidentification with generative neural networks
**Institution:** University of Ljubljana, Faculty of Computer and Information Science
**Supervisor:** Peter Peer, Vitomir Štruc
**URL:** https://repozitorij.uni-lj.si/IzpisGradiva.php?id=152341&lang=eng
**Link description:** description and PDF
**Contact email:** peter.peer@fri.uni-lj.si

**Abstract:**
Advancements in image-based biometrics and the increasing reliance on facial data have raised concerns regarding privacy protection and the potential misuse of personal information. Face deidentification techniques have emerged as a promising approach to mitigate privacy risks while preserving data utility. This thesis investigates the application of generative neural networks for facial synthesis to achieve effective face deidentification while maintaining the usefulness of the data for subsequent biometric analysis. The primary objective of this research is to develop novel techniques for face deidentification using generative neural networks. By leveraging generative deep learning algorithms, realistic synthetic faces are generated, which substitute the source facial features while preserving essential non-identity-related characteristics. Privacy protection is a critical aspect of this research, with a focus on deidentifying facial images to prevent unauthorized identification of individuals. Various techniques such as face swapping, the utilization of formal privacy mechanisms, preservation of facial attributes, and identity suppression are explored to ensure that the synthesized faces remain untraceable while maintaining their realistic appearance and data utility for further analysis. Furthermore, the thesis addresses the challenges of evaluating the effectiveness of face deidentification techniques in terms of both privacy protection and data utility. Metrics and benchmarks are presented to quantify the level of anonymity achieved while measuring the impact on data utility through the analysis of preserved facial attributes. The evaluation process involves comparing recognition accuracy, facial attribute classification performance, and other image quality metrics on deidentified face images against the source facial images. The findings of this thesis contribute to advancing face deidentification and privacy protection of biometric data, providing competitive practical solutions for face deidentification by utilizing state-of-the-art generative models.

## AIDAN BOYD - HUMAN-MACHINE TEAMING TO IMPROVE COMPUTER VISION

**Full Title:** Human-Machine Teaming to Improve Computer Vision
**Institution:** University of Notre Dame
**Supervisor:** Adam Czajka, Kevin Bowyer
**URL:** https://curate.nd.edu/show/2n49t151g06
**Contact email:** aboyd3@nd.edu

**Abstract:**
Human-machine teaming is the idea that humans and machines can provide complementary information in solving a given task such that their combination results in better performance than either individually. We implement human-machine teaming by introducing the concept of Human-AI supervision. This refers to a hypothesis that humans can provide input to train better models by guiding them towards salient information and in turn these human-aided models can help future human examiners to solve the task more effectively. This dissertation aims to address the question of how to accomplish this in the context of human visual perception and deep convolutional neural networks. This document will present a series of works that outline how to effectively guide deep learning models towards human-defined regions of saliency and thus help the models to learn more generalized features (part 1 of human-AI supervision). Finally, I will show that these human-guided models can aid future humans solving the task by supplying useful information about the sample (part 2 of human-AI supervision). By guiding our models to human-defined saliency, it avoids learning spurious features i.e. incidental features in the training data that do not generalize to the entire domain. Results show that one sample with human saliency can be equivalent to training on multiple samples without. While this idea could theoretically be applied to any domain in which humans can provide meaningful input, for this talk it will be focused on computer vision applications, specifically post-mortem iris recognition, fake iris detection, synthetic face detection and physiological abnormality detection based on chest X-ray scans.

## BO JIN - PSEUDO RGB-D FACIAL IMAGE PROCESSING

**Full Title:** Pseudo RGB-D Facial Image Processing – Towards Face Recognition And Facial Diagnosis
**Institution:** University of Coimbra
**Supervisor:** Nuno Gonçalves
**URL:** https://visteam.isr.uc.pt/publications/pseudo-rgb-d-facial-image-processing-towards-face-recognition-and-facial-diagnosis/
**Link description:** Research Center's team webpage
**Contact email:** jin.bo@isr.uc.pt

**Abstract:**
Today, face image-based applications have become widespread in fields such as security, medicine, and entertainment. Factors like lighting, pose, and facial expressions can impact the performance of these applications. Over the past decade, the development and affordability of low-cost RGB-D sensors have made it possible to obtain depth information of objects, leading researchers to tackle face recognition problems by capturing RGB-D face images. However, due to privacy restrictions, acquiring depth data from human faces remains challenging, and 2D RGB face images are still prevalent. Intelligent beings, such as humans, can use their vast experience to derive 3D spatial information from 2D scenes. Machine learning methodologies aim to solve such problems by training computers to generate accurate answers. Our research's objective is to enhance the performance of subsequent face processing tasks, such as face recognition and facial diagnosis, by obtaining depth maps directly from corresponding RGB images. We propose a pseudo RGB-D facial image processing framework that replaces depth sensors with generated pseudo-depth maps and others data-driven methods to create depth maps from 2D face images. Specifically, we design and implement a generative adversarial network model named 'D+GAN' for multi-conditional image-to-image translation with facial attributes. We validate the pseudo RGB-D facial image processing approach through experiments on face recognition and facial diagnosis using various datasets. The pseudo RGB-D facial image processing framework works in conjunction with image fusion algorithms to enhance face recognition and facial diagnosis performance. To further exploit pseudo-depth features, we ultimately propose a simulated multimodal facial image processing framework that significantly improves performance with a higher probability.

# MONITOR
# MASTER-THESES

## LENNARD MICHAEL STROHMEYER - TEST TOOLS FOR FACE IMAGE DATA IN EPASSPORTS

**Full Title:** Development and evaluation of test tools for face image data in ePassports
**Institution:** Fraunhofer IGD
**Supervisor:** Arjan Kuijper, Olaf Henniger
**Contact email:** olaf.henniger@igd.fraunhofer.de

**Abstract:**
The ISO/IEC 39794 series of standards specifies new, extensible biometric data interchange formats based on ASN.1 (Abstract Syntax Notation One), yielding binary tag-length-value encodings. According to ICAO's timeline, from 2026 onwards, newly issued electronic passports (ePassports) may use the new data formats, and ePassport inspection systems must be able to handle them. From 2030, all newly issued ePassports must use the extensible formats. Before roll-out, the new types of ePassports and inspection systems must be systematically tested. This thesis develops prototype tools for tests regarding the new face image data interchange format.

## DADI MAICHOL - HUMAN EXAMINER SUPPORT TOOL FOR IMAGE MANIPULATION DETECTION

**Full Title:** Design and development of a human examiner support system for the detection of manipulated images
**Institution:** University of Bologna
**Supervisor:** Annalisa Franco
**Contact email:** annalisa.franco@unibo.it

**Abstract:**
The purpose of this thesis is to create a tool that can help human examiners in identifying manipulated images to prevent attacks on automatic face verification systems. In particular, geometric distortions, digital beautification and face morphing are considered. Several measures, inspired by the FISWG document on the manual face morphological analysis are implemented.

## DHARSHINI THARMARAJAN - SENTIMENT ANALYSIS TO DETECT PREDATORY CONVERSATIONS

**Full Title:** Sentiment analysis to detect predatory conversations
**Institution:** NTNU
**Supervisor:** Patrick Bours
**Contact email:** patrick.bours@ntnu.no

**Abstract:**
The rapid increase in children's internet usage for activities such as gaming, video streaming, socializing, and education has raised serious concerns about their vulnerability to online predators. In 2022 alone, 32 million reports of suspected online child sexual abuse cases were documented. The anonymity provided by the internet creates an environment where malicious individuals can easily abuse children for sexual exploitation. In light of the emotional instability often exhibited by predators, this master's thesis focuses on detecting predatory conversations through sentiment analysis on an unlabeled real-life dataset obtained from a gaming platform. This study adopts a two-stage approach. In the first stage, the utilization of k-means clustering combined with anticipation, joy, and positive and negative sentiment features enables the identification of a group of conversations that potentially contain a higher degree of predatory content. This group serves as the foundation for establishing a ground truth. In the second stage, 50 predatory conversations and 50 normal are extracted from the previously identified group for training classifiers. SVM classifiers are trained using GSF, IF, and CF, extracted from the conversations without any preprocessing. Moreover, ensemble classifiers are also evaluated for performance. Promising results are obtained using an SVM classifier with GSF, achieving a precision of 0.77, a recall of 0.94, an F2-score of 0.89, and an accuracy of 0.81. Ensemble classifiers did not provide any better performance compared to the best results. These findings demonstrate the capability of sentiment analysis to detect predatory conversations within real-life gaming datasets. By incorporating sentiment and emotional markers, along with appropriate feature selection and classifier training, the identification of predatory conversations can be effectively achieved.

## NICOLAI NAKKEN - IDENTIFYING KEYS USING ACOUSTIC EMANATIONS FROM KEYSTROKES

**Full Title:** Identifying keys using acoustic emanations from keystrokes
**Institution:** NTNU
**Supervisor:** Patrick Bours
**Contact email:** patrick.bours@ntnu.no

**Abstract:**
Previous research has proved it possible to reconstruct text typed on a keyboard by analyzing the acoustic emanations. This indicates a serious security vulnerability, and the need for further understanding. In this master thesis we present our own system and compare our method and results with previous work. Data was collected using four microphones placed around a keyboard, cross-correlation is then used to measure the time-difference of arrival measurements which are used to identify which key was pressed. We propose a new method of mitigating errors from the cross-correlation functions and our test showed a significant improvement. Our system was made with future research in mind, allowing for improvements and testing of alternate methods. After struggling to get a working system using a data set collected by another student, we decided to invest a lot of time and effort in collecting our own, something future researchers also can take advantage of. In the end our system was able to identify what key was pressed 87.1\% of the time. If future research takes advantage of spell checking and grammar, the accuracy can be easily improved.

## ALEXANDER FAARUP CHRISTENSEN - DIGITAL FACE MANIPULATION DETECTION

**Full Title:** Ensemble Learning for Generalized Digital Face Manipulation Detection
**Institution:** Technical University of Denmark (DTU)
**Supervisor:** M. Ibsen (h_da), C. Rathgeb (h_da), C. Busch (h_da), C. D. Jensen (DTU)
**Contact email:** mathias.ibsen@h-da.de

**Abstract:**
This thesis explores the use of ensemble learning techniques for the detection of manipulated digital faces. The research aims to develop an approach to generalize digital face manipulation detection by using ensemble learning methods to combine the predictions of multiple classifiers in a hierarchy model. The study used various datasets of malicious and benign manipulated, and bonafide digital face images. Many of the manipulated face images and all of the bonafide images were taken from existing databases, with proper references, while the rest were generated using OpenCV and custom functionality. The results showed that the ensemble learning approach achieved good recall, precision, as well as APCER and BPCER. The research has significant implications for the detection of digital face manipulation in various applications, including forensics and security. The study demonstrates the effectiveness of ensemble learning techniques for detecting digital face manipulation and highlights the importance of using a generalized approach to achieve higher accuracy and reliability in the detection process. The results show that while using an ensemble model for PAD yields prominent results, there is still a long way to go before the model can be used in commercial options.

## VINAY PRADHAN - ENHANCING FACE-RELATED BIOMETRIC TECHNIQUES

**Full Title:** Enhancing Face-related Biometric Techniques using a Novel Dataset
**Institution:** Hochschule Darmstadt
**Supervisor:** Christoph Busch and Marcel Grimmer
**Contact email:** marceg@ntnu.no

**Abstract:**
The field of biometrics research is growing in importance in the modern world. Advancements in biometric techniques change everyday life: from face or fingerprint unlock for smartphones to iris recognition for advanced security systems. To continue the rapid growth of this research field, it is necessary to identify and utilise new data sources which might further accelerate or improve development. This thesis focuses on the investigation and development of a novel dataset of facial images, which would open a new data source for new initiatives. The impact of the proposed dataset on face-related biometric techniques, such as Face Age Estimation or Face Age Progression, will be evaluated. While the data collection and evaluation presents the core of this thesis, ethical and legal considerations will also be noted to ensure that a scalable dataset is presented for future researchers.

## KACPER M. ZYLA - HAND-BASED BIOMETRICS FOR FORENSIC ANALYSIS

**Full Title:** Hand-based Biometrics for Forensic Analysis
**Institution:** Technical University of Denmark
**Supervisor:** Prof. Dr. Christian Rathgeb, Dr. Lazaro Janier Gonzalez-Soler, and MsC Daniel Fischer
**Contact email:** lazaro-janier.gonzalez-soler@h-da.de

**Abstract:**
Despite the progress made in face and fingerprint, in some forensic scenarios it is not possible to successfully acquire such biometric characteristics. Therefore, the need for other ways of performing biometric recognition is of utmost importance to the research community. Hand anatomy is the key to determine the individuality of hand-based biometrics. The thesis investigated the performance of hand-based biometric recognition systems in forensic investigation scenarios. Three state-of-the-art systems were selected and evaluated over several experiments. In addition, three hand image datasets of varying complexity were used to evaluate the accuracy of biometric recognition in conditions ranging from ideal to challenging. The results presented in this Thesis showed that, while the tested systems can operate reliably in controlled data, their performance was significantly worse in uncontrolled scenarios. The experiments conducted in this thesis indicated that hand position and rotation, as well as image background, can significantly affect the accuracy of the tested models. This report concluded with a proposal for further studies that could counteract these factors and other future research perspectives.

## MILAN ŠALKO - SECURITY IMPLICATIONS OF DEEPFAKES IN FACE AUTHENTICATION

**Full Title:** Security Implications of Deepfakes in Face Authentication
**Institution:** Brno University of Technology
**Supervisor:** Anton Firc
**URL:** https://www.vut.cz/en/students/final-thesis/detail/141060
**Contact email:** isalko@fit.vut.cz

**Abstract:**
Deepfakes, media generated by deep learning that are indistinguishable to humans from real ones, have experienced a huge boom in recent years. Several dozen papers have already been written about their ability to fool people. Equally, if not more, serious, may be the problem of the extent to which facial and voice recognition systems are vulnerable to them. The misuse of deepfakes against automated facial recognition systems can threaten many areas of our lives, such as finances and access to buildings. This topic is essentially an unexplored problem. This thesis aims to investigate the technical feasibility of an attack on facial recognition. The experiments described in the thesis show that this attack is not only feasible but moreover, the attacker does not need many resources for the attack. The scope of this problem is also described in the work. The conclusion also describes some proposed solutions to this problem, which may not be difficult to implement at all.

## AJAY MATHEW JOSEPH - HUMAN ACTIVITY RECOGNITION

**Full Title:** Investigating vision transformers for human activity recognition from skeletal data.
**Institution:** University of Twente
**Supervisor:** Luuk Spreeuwers
**URL:** https://essay.utwente.nl/94291/
**Link description:** Investigating vision transformers for human activity recognition from skeletal data.
**Contact email:** l.j.spreeuwers@utwente.nl

**Abstract:**
Transformers are increasingly being used for different kinds of applications these days. Recent works show that vision transformers can also demonstrate great capacity in solving Human Activity Recognition tasks based on skeletal trajectories. However, there are still certain aspects of them that are left unexplored, with respect to the input representation as well as the model architecture. We investigate two aspects of the problem: first, we use skeletal keypoint trajectories as inputs which are decomposed locally as well as globally. Secondly, we introduce convolutional learning in to transformers by using tubelet embeddings which we assume could extract better spatio-temporal information. We inspect our model on two different datasets, NTURGB+D 120 and HR-Crime. We observe that decomposing the keypoints globally and locally does not improve the performance. We also observe that incorporating a tubelet embedder to a simple transformer architecture gives similar results as the baseline results with significantly lesser computational costs. We also discuss the limitations of our work and what could be done to improve it.

## MAGNUS FALKENBERG - GENERATION OF SYNTHETIC CHILDREN FACES

**Full Title:** Generative Adversarial Networks for Generation of Synthetic Children Faces
**Institution:** Technical University of Denmark (DTU)
**Supervisor:** M. Ibsen (h_da), C. Rathgeb (h_da), C. D. Jensen (DTU)
**URL:** https://dasec.h-da.de/2023/05/magnus-falkenberg-and-anders-bensen-ottsen-successfully-defended-their-master-thesis-on-generative-adversarial-networks-for-generation-of-synthetic-children-faces/
**Link description:** Completed thesis announcement
**Contact email:** mathias.ibsen@h-da.de

**Abstract:**
Biometric systems, and especially facial recognition systems, have become ubiquitous in our daily lives, serving as a reliable means of authentication for personal devices. Recently, deep learning has significantly improved the performance of facial recognition technology, albeit these approaches are dependent on the quality and quantity of the data used for training. As such, the verification performance of these systems on children is reported as subpar as there exists no large-scale unbiased database of children's faces, due to privacy concerns. However, automatic recognition of children from faces has numerous applications, including the potential to find missing or kidnapped children or analyze child sexual abuse material. Therefore, this thesis aims to address the need for a database of children's faces by using generative adversarial networks (GANs) and face age progression (FAP) models to synthesize a realistic dataset. To generate high-quality adult and corresponding child faces, the thesis performs an evaluation of various state-of-the-art FAP methods, considering several criteria, including the preservation of subject identity across ages. The final solution involves a software pipeline consisting of multiple steps and models. The pipeline initially utilizes StyleGAN3 to sample adult subjects, which are subsequently progressed to children of varying ages using InterFaceGAN, enabling direct manipulation of subjects in the StyleGAN3 latent space. Intra-subject variations, such as facial expression and pose, are created by also manipulating the subjects in their latent space. Additionally, the pipeline allows to evenly distribute the races of subjects, allowing to generate a balanced and fair dataset with respect to race distribution. Using the pipeline, a database was created, consisting of 1652 subjects and a total of 188,832 images. The significant number of images is due to each subject being present at various ages and with many different intra-subject variations. The thesis evaluates the performance of various facial recognition systems on the synthetic database and compares the results of adults and children at different ages. The study reveals that children consistently perform worse than adults, on all tested systems, and the degradation in performance is proportional to age. Additionally, the study uncovers some biases in the recognition systems, with Asian and Black subjects and females performing worse than White and Latino Hispanic subjects and males. Overall, this thesis provides valuable insights into the performance of facial recognition systems on children and highlights the need for unbiased, diverse data sets to train these systems. The synthetic database created through this work can serve as a valuable resource for researchers and practitioners in the field.

## ANA TEIXEIRA DE VISEU CARDOSO - XAI FOR INTERPRETABLE AND FAIR FACE RECOGNITION

**Full Title:** Explainable Artificial Intelligence - Getting insights from Deep Neural Networks for Interpretable and Fair Face Recognition
**Institution:** FEUP, University of Porto
**Supervisor:** Ana Filipa Sequeira
**URL:** https://hdl.handle.net/10216/153871
**Link description:** openAccess
**Contact email:** ana.f.sequeira@inesctec.pt

**Abstract:**
Human faces convey information about gender, age and ethnicity and more abstractly about a subject's emotions and social context. The capacity to identify and authenticate individuals based on their facial features currently represents the most commonly used type of data in biometric systems. Face recognition technology has evolved significantly in recent years, propelled by the proliferation of digital image data and the rise of Artificial Intelligence, which is directly linked with the development of Deep Learning methods. Deep Neural Networks are used on several fronts and achieve impressive results, even when comparing to the ones achieved by humans performing the same tasks. The remarkable Deep Learning developments carried consequences, namely the transition from understandable models into black box systems. The trade-off between good quantitative results and the fairness and transparency of a model needs to be considered. Explainable Artificial Intelligence focus on the explainability of a model and unveils certain challenges and biases that remain present, particularly racial bias. This is a complex issue with implications on both ethical and social dimensions, transcending the domain of technology. Although racial bias is currently more studied, there is still little information available on the impact on the performance of face recognition algorithms. One of the primary contributors to racial bias is the imbalance in training data, given that many datasets are predominantly composed of images from a specific ethnic group and lack in diversity. Therefore, one of the main efforts to mitigate racial bias includes creating more diverse training databases, as well as developing fair algorithms. As face recognition systems have been adopted as a powerful security tool, racial inequity can translate into social injustices and misidentifications, raising the need for awareness on this topic. This dissertation delves into the analysis and exploration of racial bias in face recognition systems. The work developed commences with a background and literature review, tracing the evolution of face recognition. The methods adopted focus on the use of race-aware databases and we aim to evaluate if the face recognition model used performs differently with four racial groups (Caucasian, African, Asian and Indian) under the same conditions. To investigate racial bias, especially intra-racial bias, various experiments were performed, starting with an analysis of the effects that image transformations have on a particular race. Moreover, gradient maps were generated for all races in the same layers of the network, allowing an analysis of the regions of interest in the input images. We performed practical experiments on neural network activations to look for a possible connection between human face recognition of subjects from other races and automatic face recognition evaluated on a race-aware dataset. As deep neural networks cannot be evaluated over time, the analysis made focused on how data flows through the network layers in a specific order. We calculated metrics such as mean and standard deviation from the neural network activation values extracted from the network's layers and the results were compared between races. At last, using the neural network feature maps generated from specific layers, we tested the separability of racial groups. Even though various ideas were pursued, the experiments did not present a clear and straightforward conclusion on racial bias and the reasoning behind it. However, it is mandatory that this topic keeps on being studied and addressed. Moreover, in terms of future work, it may be interesting to focus on some racial bias mitigation techniques and, by adding synthetic bias to the data, measuring its quantitative impact on the tests performed in this dissertation.

## SOFIA BOSCH PASTOR - DETECTING THE DATA EMPLOYED TO TRAIN

**Full Title:** Catch Me If You Can: Detecting the Data Employed to Train Deep Neural Networks
**Institution:** Universidad Autonoma de Madrid
**Supervisor:** Aythami Morales Moreno
**URL:** https://repositorio.uam.es/handle/10486/700636
**Link description:** UAM repository
**Contact email:** aythami.morales@uam.es

**Abstract:**
Face recognition algorithms are trained with huge amounts of data with slight control over what is happening during training and with which data was used. In this work, we consider the potential risk to personal privacy that may suppose machine learning systems by using specific data for training process. For this reason, and focusing on the representation of feature extracted from facial analysis technologies, we seek to learn the representation of features extracted from samples used for training and samples not used during training. The main objective of this Mater Thesis is to study and develop technology to detect whether a specific image was used during the training process of a Machine Learning model. With this aim, we carried out a review of the State of the Art in the field of face recognition, as well as a research on Membership Inference Attacks (MIAs) in which Machine learning models are vulnerable. MIAs aim to infer whether a data record was used to train a target model or not. As MIAs on ML models can directly lead to a privacy breach. Following this research, state-of-the-art methods for learning feature representations and activations in a popular pre-trained face recognition model are proposed. In our experiments we study the extraction of facial features and representations obtained by a pre-trained model used for face recognition. Then with a supervised learning we are going to study the capability to distinguish between a database used for training and not used for training. Finally, we explore whether the model is truly learning identities or images from the training database. Furthermore, an experiment was proposed to examine the network's ability to differentiate between specific databases or individuals within the database. In conclusion, this Master's thesis presents a comprehensive analysis of face recognition model. The research highlights the significance of distinctive facial feature extraction for the detection of the training data. The findings contribute to the knowledge about how Deep Neural Network works and what happened with the training data of the face recognition models. In that way, it could be used to protect the privacy for example for people that don't allow the use of their faces.

## FELIX GARCIA FUNK - FINGER VEIN IMAGE QUALITY ASSESSMENT

**Full Title:** Finger vein image quality assessment based on mated comparison score prediction
**Institution:** Fraunhofer IGD
**Supervisor:** Arjan Kuijper, Olaf Henniger
**Contact email:** olaf.henniger@igd.fraunhofer.de

**Abstract:**
Successfully assessing the quality of finger vein images is an important step during image acquisition and can be used to improve the biometric recognition performance. Current methods achieve such quality assessment by training a machine learning system against predefined quality labels. The system approximates the targets and is thereby limited by the labels in use. Therefore, the assignment of quality labels plays an important role for the performance of the quality assessment and provides an additional source of error. No commonly agreed definition for finger vein image quality exists, however, making the assignment of quality labels a task on its own. Because many systems focus mostly on the machine-learning part, unsophisticated practices such as human assignment of quality labels are still common. This work presents an alternative to the explicit assignment of quality labels. The proposed method uses mated comparison scores as training targets and defines the quality assessment system implicitly. The necessity of quality labels is avoided and the model can freely adapt to the underlying data. Because only a fraction of the available finger vein image datasets represents low quality and common data augmentation schemes do not fit the circumstances of the approach, a new method to counter data imbalance is investigated as well. It utilizes image generation performed by a conditional generative adversarial network and produces realistic synthetic finger vein images to augment the training data with more low quality images.

## SIMEN MELLEBY AARNSETH - DETECTING CYBER GROOMING

**Full Title:** Fine tuning BERT for detecting cyber grooming in online chats
**Institution:** NTNU
**Supervisor:** Patrick Bours / Sushma Venkatesh
**Contact email:** patrick.bours@ntnu.no

**Abstract:**
This thesis will look into how cyber grooming may be detected through the natural language processing model BERT, with an emphasis on the use of abbreviations and slang present in the chats. To investigate this, several BERT models were trained. These models where trained and tested on different data sets consisting of a varying amount of abbreviations and slang expressions. Through this, BERTs ability to detect cyber grooming based on the prevalence of abbreviations and other informal language forms could be assessed. The findings from this process indicated that BERT was able to detect cyber grooming at a similar rate between data sets where the prevalence of abbreviations and slang was much higher in one compared to the other. This indicated that BERT possesses the ability to understand language quite well despite it being in a more informal form.

## JOANA PIMENTA - IMPACT OF IMAGE CONTEXT FOR DEEP MORPHING DETECTION

**Full Title:** Impact of Image Context for Deep Morphing Detection
**Institution:** University of Coimbra
**Supervisor:** Nuno Gonçalves
**URL:** https://visteam.isr.uc.pt/publications/impact-of-image-context-for-deep-morphing-detection/
**Link description:** Research center's team webpage
**Contact email:** nunogon@deec.uc.pt

**Abstract:**
The use of the face as a way to identify and verify an individual's identity has significantly impacted the expansion of biometric systems, particularly face recognition systems, as a security measure. However, the human face is extremely susceptible to manipulation, making the systems highly vulnerable to threats and attack attempts. Face morphing is one of the most concerning attacks since it allows to obtain an image of an individual that appears to be real but, in fact, does not exist. Furthermore, the resulting image can be easily confused with the faces of two or more individuals, as it incorporates a combination of their facial characteristics. This allows, for instance, an attacker to impersonate another person and gain unauthorized access to sensitive information or systems. For all these reasons, the ability to detect these attacks is crucial and has been the subject of intensive study by researchers. Currently, most of these techniques use deep learning algorithms, which have demonstrated effectiveness in realistic scenarios. In this dissertation, the main goal is to investigate the influence of image context on the detection of face morphing attacks in the particular case of deep learning algorithms. In that regard, it is proposed to analyze the impact of the image alignment settings on the detection of these attacks. This is motivated by the fact that the face alignment procedure directly influences the interconnections between the face contour and image context. Thus, effective detection can be achieved by obtaining optimal alignment conditions.

## MARK TREBELJAHR - BIOMETRIC TEMPLATE PROTECTION

**Full Title:** Biometric template protection by GAN-based replacement of original fingerprints
**Institution:** Otto-von-Guericke University Magdeburg
**Supervisor:** Dr.-Ing. AndreyMakrushin, Prof. Dr.-Ing. Jana Dittmann
**Contact email:** andrey.makrushin@ovgu.de

**Abstract:**
Fingerprints are a highly efficient medium for fast and reliable identity authentication. However, strict security standards apply to this biometric data. Once compromised, either through loss or theft, the data becomes useless for personal identification and enables potential identity theft. This thesis introduces and implements a concept that merges the work of Cappelli et al. [17] and Karras et al. [20], generating cancelable fingerprints based on genuine print images. These are intended for identity verification, discerned from authentic fingerprints by their ability to be updated using the algorithm presented here in case of loss. This allows the continued use of the original biometric data, while rendering the compromised print unusable for possible identity theft. A comparative analysis of the synthesized fingerprints shows a significant difference in terms of actual identity, although with a classification accuracy of only 70%. Furthermore, the ability to update the corresponding fake biometric data is demonstrated, making the supposedly lost prints truly worthless.

## KEVIN BARHAUGEN - UNSUPERVISED ANOMALY DETECTION

**Full Title:** Unsupervised Anomaly Detection
**Institution:** NTNU
**Supervisor:** Patrick Bours
**Contact email:** patrick.bours@ntnu.no

**Abstract:**
This research aims to explore if unsupervised anomaly detection can be used to detect anomalies in conversations used in a highly biased dataset. A web chat based dataset from the Børns Vilkår company was received in order to preprocess the text messages, cluster them together and find potential anomalies of any kind in the dataset. The results managed to highlight conversations based on different languages as anomalous, but did not manage to highlight differences in the conversations' content. Based on these results, the conclusion to detecting anomalies in conversation used in highly biased datasets is therefore inconclusive. Recommended future work is to implement a multilingual model that are able to handle multiple languages in a dataset, to find more meaningful anomalies, based on the content of the conversations in the dataset.

## AZIZ FAGLAGIC - UNMASKING THE CHEATING STUDENT

**Full Title:** Unmasking the cheating student
**Institution:** NTNU
**Supervisor:** Patrick Bours
**Contact email:** patrick.bours@ntnu.no

**Abstract:**
Unlike plagiarism detection, where multiple tools have developed over recent decades, as contract cheating is based on students purchasing assignments from third-parties that are original, traditional plagiarism detection tools remain insufficient to detect contract cheating. Unmasking is a technique which can determine if two texts were written by the same author. This technique will be applied to short text, with the aim to see whether it is an appropriate model for countering contract cheating. This involves developing an unmasking software framework which analyzes given texts and determines whether they are from the same author or not. This will help counter academic dishonesty primarily in education and academic institutes. Through this study, the unmasking shows that it performs better on longer texts than short texts. Therefore, there is a need for further investigation for short text unmasking.

## PEDRO GONÇALVES - VERIFICATION OF THE COMPLIANCE OF ICAO REQUIREMENTS

**Full Title:** Partial Automatic Verification of the Compliance of ICAO requirements for Portraits
**Institution:** University of Coimbra
**Supervisor:** Nuno Gonçalves
**URL:** https://visteam.isr.uc.pt/publications/partial-automatic-verification-of-the-compliance-of-icao-requirements-for-portraits/
**Link description:** Research center's team webpage
**Contact email:** nunogon@deec.uc.pt

**Abstract:**
Biometric verification plays an extremely important role in today's context of international travel and identification of humans. In this regard, the International Civil Aviation Organization (ICAO) has created a document based on the ISO/IEC 19749-5 standard, aimed at ensuring compliance with the photographic requirements of facial images for use in official documents. However, this verification process is still largely carried out manually by qualified professionals, an approach that is not only subjective but also time-consuming. There is a growing need to develop automatic verification systems for this purpose. This dissertation seeks to address this challenge by exploring approaches based on the use of neural networks – YOLOv8 and ResNet-50 – to verify a facial photograph according to ICAO requirements, specifically those related to the verification of prescription glasses. Both architectures were trained and tested using a dataset resulting from a partnership between the ISRCoimbra (Institute of Systems and Robotics) and the INCM ("Imprensa Nacional Casa da Moeda") as part of the FACING2 project, which aims to create a dataset of facial photographs to assess compliance with ICAO requirements. The proposed solutions were developed based on the classification models resulting from the use of YOLOv8 and ResNet neural networks, with the aim of automating the verification of ICAO requirements. Finally, the results obtained are discussed and compared with a method in the literature called ICAONet. The results are quite promising, as they are on par with some of the best results published by this methodology, suggesting that neural network-based approaches have the potential to significantly improve the efficiency and accuracy of biometric verification in accordance with ICAO standards.

## JAN LUO TANG - EARLY DETECTION OF CYBERGROOMING CONVERSATIONS

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

**Abstract:**
The issue of cybergrooming has gained more attention as more people engage with one another online. To address this issue, preventative mechanisms that detect cybergrooming attempts in online conversations could be implemented. In this thesis, a method for early detection of cybergrooming conversations was explored. A new data set containing conversations from different online games aimed at children was analyzed and labeled. Using this data, a novel risk update mechanism was developed that continuously evaluates the risk of ongoing conversations by looking at individual messages. This mechanism had several adjustable parameters, which, together with a risk threshold, were finetuned for classification performance and earliness. Validation methods were then used to evaluate the performance of the system. The results were promising, both with regard to correct classification and detecting cybergrooming attempts early in ongoing conversations. This thesis has, through the obtained results, demonstrated that a risk-based system could be used for the early detection of cybergrooming conversations.

## MORTEN BJERRE - AGE-EG3D

**Full Title:** Face Age Progression Based on Generative Adversarial Networks
**Institution:** Norwegian University of Science and Technology
**Supervisor:** Christoph Busch and Marcel Grimmer
**URL:** https://github.com/johndoe133/eg3d-age/tree/main
**Link description:** Official Repository
**Contact email:** marceg@ntnu.no

**Abstract:**
It is a complicated endeavour to change an individual's facial appearance such that their face image would be an accurate estimate of the individual's likeness up to decades in the future or past. To achieve that, one needs to create a realistic, high-quality face image of the correct age while also maintaining the person's identity, all from one image. Accomplishing this is made even more difficult by aging being a highly individual process, which varies greatly based on lifestyle and genetics. Current works are limited to creating face images from the original viewing angle, which is not ideal. This work aims to use the recent advances in generative adversarial networks (GANs) and their application both in face aging and generating 3D images from single 2D input images to address all these problems. This is accomplished by extending the existing EG3D network, one of the most advanced state-of-the-art works on 3D GANs, and appending the age condition to the input and augmenting the loss with identity preservation loss. The end product is age-EG3D, which can create wholly synthetic photorealistic face images with a custom target age and viewing angle while maintaining the identity of the subject. Age-EG3D achieves an impressive mean absolute error (MAE) of 4.1 years for synthetic images. It also enables age simulation on real face images with an MAE of 7.9.

## SIGNE BEATHE THRANE-NIELSEN - UNMASKING THE CHEATING STUDENT

**Full Title:** Unmasking the Cheating Student
**Institution:** NTNU
**Supervisor:** Patrick Bours
**Contact email:** patrick.bours@ntnu.no

**Abstract:**
Technology has enabled students to submit and write their assignments and exams online, making detecting cheating challenging. One form of cheating is called contract cheating, which is when a student gets a third party to answer an exam or write an assignment on their behalf. The student then submits the work as their own. This has become a huge problem as traditional cheating tools are not equiped to handle contract cheating. This thesis investigated if it is possible to detect contract cheating on short texts. Three different methods for detecting contract cheating were developed and tested using three datasets, one with long text and two with short text. All three methods used character- and word-level n-grams as features. The unmasking method applied svm, 10-fold cross-validation, and a "bag-of-words" approach for chunk allocation. The best result on short texts achieved an accuracy of 54.03%, while long texts obtained an accuracy of 60.99% using word-level bigrams. The Relative measure method based on keystroke dynamics gave an accuracy of 31.30% when testing with long texts. In contrast, short texts gave an accuracy of 50.72%. Absolute measure, also based on keystroke dynamics, achieved the best results on longer texts. Several alternations were applied to the Absolute measure method, including a new distance measure, texts where all stop words were removed, texts where only stop words were kept, and using the Linguistic Inquiry and Word Count (LIWC)1 software. The highest accuracy obtained with long texts was 90.43% when only the new distance measure was considered. With short texts, the highest accuracy was 71.44% when using the new distance measures and texts only consisting of stop words. Regardless of whether the original Absolute measure or the new alterations were used, the best results were obtained using character-level bigrams as feature sets.

## YULING JIANG - PATCH-BASED MORPHING ATTACK DETECTION

**Full Title:** Patch-Based Morphing Attack Detection
**Institution:** Universiteit Twente
**Supervisor:** Luuk Spreeuwers
**URL:** https://essay.utwente.nl/97090/
**Link description:** Patch-Based Morphing Attack Detection
**Contact email:** l.j.spreeuwers@utwente.nl

**Abstract:**
The morphing attack poses a significant threat to face recognition systems, as it undermines the unique link between identity and identification documents. Therefore, the need for morphing attack detection is imperative. In this paper, we proposed a novel patch-based morphing attacks detection approach. The facial regions from the images were cropped and divided into 30 patches. This methodology facilitates a straightforward expansion of the dataset size. We conducted a comprehensive analysis comparing different combinations of feature extraction networks and score fusion mechanisms. The findings demonstrate that the utilization of Se_Resnet50 as the feature extractor, combined with either the average or machine learning score fusion method, produces satisfactory results during the test phase. In particular, the D-EER for intra-dataset tests is 0%, and the highest D-EER observed for cross-dataset tests is merely 12.1%. However, when conducting cross-dataset testing, morphs generated with STYLEGAN2 exhibit an exception to this trend. Subsequently, extensive experiments with the optimal combination were conducted to investigate the influence of various training settings on the outcomes. The findings unveiled that when subjected to images generated by STYLEGAN2 from distinct datasets, a model exclusively trained on STYLEGAN2-generated images exhibited enhanced capabilities in generalization. Furthermore, there are certain similarities in the artifacts observed in both landmark-based and GAN-based morphed images.

## MARIE SOMNEA HENG - EARLY SOFT BIOMETRIC VOICE RECOGNITION

**Full Title:** Early Soft Biometric Voice Recognition
**Institution:** NTNU
**Supervisor:** Patrick Bours and Matus Pleva (TUKE)
**Contact email:** patrick.bours@ntnu.no

**Abstract:**
Adults who pretend to be children can pose a threat to children by providing their wrong age on communication platforms to approach children online. Concerning this topic, studies have been conducted to investigate the human voice regarding age classification. In this master's thesis, a training model prototype was used to classify voices into three groups: child, adult, and transitional age group. The inclusion of a transitional age group in the classification helps to consider the diverse stages of individual voice development. The classification model prototype was trained using the Samrómur dataset. Testing was conducted using a sample from the Common Voice dataset and the "Children speech recording" dataset. The available information did not include details about the distinction between their labelled verified and non-verified audio files. Therefore, two versions of the Samrómur dataset were created for training the model: one with only verified datasets and another with the complete dataset. The model trained with the verified dataset achieved an accuracy of 95.23%, while the model trained with the complete dataset achieved an accuracy of 90.68%. Both showed signs of an overfitted model either in their loss curve or in the model testing with the other datasets. Maintaining a high accuracy is crucial for practical applicability. A calculation demonstrated that classifying three pieces of three-second audio theoretically results in a 99% accuracy. Therefore, based on the trained model, the speaker's voice can be classified as early as seven seconds. This calculation considers the trimming method, where each subsequent trim overlaps one second onto the previous piece.

## DENNIS HOFTIJZER - SHORTCUT LEARNING

**Full Title:** Language-Based Augmentation to Address Shortcut Learning in Object-Goal Navigation.
**Institution:** Universiteit Twente - Zilverling Service Desk
**Supervisor:** Luuk Spreeuwers
**URL:** https://essay.utwente.nl/94505/
**Link description:** Language-Based Augmentation to Address Shortcut Learning in Object-Goal Navigation.
**Contact email:** l.j.spreeuwers@utwente.nl

**Abstract:**
Deep Reinforcement Learning (DRL) has shown great potential in enabling robots to find certain objects (e.g., 'find a bed') in environments like homes or schools. This task is known as Object-Goal Navigation (ObjectNav). Although DRL has shown impressive results, the simulators are key and may be biased or limited. This creates a profound risk of shortcut learning i.e., learning a policy tailored to specific visual details of training environments. Therefore, in this work, we aim to deepen our understanding of shortcut learning in ObjectNav, its implications and propose a solution. We design an experiment for inserting a shortcut bias in the appearance of training environments. As an example, we associate room types to specific wall colors (e.g., bedrooms have green walls), and observe poor generalization of a SOTA ObjectNav method to environments where this is not the case (e.g., bedrooms now have blue walls). Further analysis shows that shortcut learning is the root cause: the agent learns to navigate to target objects, by simply searching for the associated wall color of the target object's room. To solve this, we propose Language-Based Augmentation (L-B). Our key insight is that we can leverage the multimodal feature space of a Vision-Language (V-L) model to augment visual representations directly at the feature-level, requiring no changes to the simulator, and only an addition of one layer to the model. Where the SOTA ObjectNav method's success rate drops 69%, our proposal has only a drop of 23%

## DURITA KVILT JÓNSDÓTTIR - ADVANCED HAND-BASED BIOMETRICS FOR FORENSICS

**Full Title:** Advanced Hand-based Biometrics for Forensics
**Institution:** Technical University of Denmark
**Supervisor:** Prof. Dr. Christian Rathgeb, Dr. Lazaro Janier Gonzalez-Soler, and MsC. Daniel Fischer
**Contact email:** lazaro-janier.gonzalez-soler@h-da.de

**Abstract:**
In many forensic scenarios criminals often attempt to conceal their identity by covering their face and other distinctive features. In such cases, the material can however reveal other unique features which can be used for identification, such as the hand(s). Many state-of-the-art (SOTA) hand-based biometric systems can accurately identify individuals in constrained environments. Nevertheless, for forensic investigations, the environment is often unconstrained, and the identification becomes considerably more challenging, resulting in a decrease in accuracy. In this project, different ways of enhancing the performance of SOTA hand-based identification models in unconstrained environments are explored. This is done by determining the performance improvements of implementing hand-alignment, fusion and loss function optimization. Multiple hand-alignment methods are explored, including a simple rotation, an affine transformation and a palmprint extraction. Furthermore, several fusion techniques are evaluated, including both score level and rank level approaches, while only one alternative loss function was evaluated, namely the additive angular margin loss. The results of this study highlight that applying hand-alignment and fusion techniques can improve the identification rate of the SOTA hand-based identification models. Specifically, the simple hand-alignment and the score level fusion with Weibull normalization emerge as the superior methods. Combining both hand-alignment and fusion techniques, reports the highest absolute performance improvement, as much as 18.8\%. However, the results obtained from implementing the additive angular margin loss function are inconclusive, as they do not consistently improve performance. Despite optimizing the SOTA models, the identification rate in unconstrained environments is far from optimal. Therefore, future research is required to determine if there exist other methods leading to even higher performance improvements. This includes exploring other hand-alignment methods, image enhancement and using large-scale data.

## CHIARA-MARIE ZOK - MULTIBIOMETRIC HOMOMORPHIC TRANSCIPHERING

**Full Title:** Efficient Multibiometric Two Factor Authentication Using Homomorphic Transciphering
**Institution:** Hochschule Darmstadt
**Supervisor:** Christoph Busch, Anamaria Costache, Pia Bauspieß
**URL:** https://dasec.h-da.de/2023/08/chiara-marie-zok-successfully-defended-her-masters-thesis-on-efficient-multibiometric-two-factor-authentication-using-homomorphic-transciphering/
**Link description:** Completed thesis announcement
**Contact email:** pia.bauspiess@ntnu.no

**Abstract:**
Biometric authentication is used in day-to-day life and in highly sensitive situations such as border control. Therefore, biometric features are extracted from samples and stored in biometric templates. Previous work has proven that samples can be reconstructed from templates. Therefore, template protection using Fully Homomorphic Encryption (FHE) has been shown to be effective in preventing such attacks. However, FHE is too resource intensive in systems where one participant has significantly low computational power. A further security risk is the low entropy for single biometric features. Homomorphic transciphering in combination with multibiometrics has the potential to solve both problems at the same time. Homomorphic transciphering is the process of transforming a symmetric ciphertext in a homomorphically encrypted ciphertext. In this thesis, two-factor authentication is achieved through transciphering. It is shown how multiple features of varying lengths and data types can be compared in the encrypted domain.

## ERIC JENSEN - AGE-EG3D

**Full Title:** Face Age Progression Based on Generative Adversarial Networks
**Institution:** DTU and NTNU
**Supervisor:** Christoph Busch and Marcel Grimmer
**URL:** https://github.com/johndoe133/eg3d-age/tree/main
**Link description:** Official Repository
**Contact email:** christoph.busch@ntnu.no

**Abstract:**
It is a complicated endeavour to change an individual's facial appearance such that their face image would be an accurate estimate of the individual's likeness up to decades in the future or past. To achieve that, one needs to create a realistic, high-quality face image of the correct age while also maintaining the person's identity, all from one image. Accomplishing this is made even more difficult by aging being a highly individual process, which varies greatly based on lifestyle and genetics. Current works are limited to creating face images from the original viewing angle, which is not ideal. This work aims to use the recent advances in generative adversarial networks (GANs) and their application both in face aging and generating 3D images from single 2D input images to address all these problems. This is accomplished by extending the existing EG3D network, one of the most advanced state-of-the-art works on 3D GANs, and appending the age condition to the input and augmenting the loss with identity preservation loss. The end product is age-EG3D, which can create wholly synthetic photorealistic face images with a custom target age and viewing angle while maintaining the identity of the subject. Age-EG3D achieves an impressive mean absolute error (MAE) of 4.1 years for synthetic images. It also enables age simulation on real face images with an MAE of 7.9.

## GARCES MALDONADO CARLOS - COMPENSATION OF CROSS-TALKS

**Full Title:** Compensation of Cross-talk in a Large Piezoresistive Sensor Array.
**Institution:** Universiteit Twente
**Supervisor:** Luuk Spreeuwers
**URL:** https://essay.utwente.nl/96347/
**Link description:** Compensation of Cross-talk in a Large Piezoresistive Sensor Array.
**Contact email:** l.j.spreeuwers@utwente.nl

**Abstract:**
Flexible resistive sensors have applications in modern devices that implement tactile sensors for pressure and force sensing. The e-Cone is a low-cost prototype device developed by the University of Twente to measure grip strength. The last version of this sensor has a high resolution of 64x128 sensor pixels. However, the sensor exhibits significant cross-talk, which adversely affects the readout of sensing pixels when multiple pixels are simultaneously pressed. To address this issue, we present an evaluation method that utilises spring mechanisms to study the behaviour of a single sensing pixel. Additionally, we propose a modification to the acquisition PCB circuit aimed at reducing the cross-talk. Finally, we introduce a machine learning approach to compensate for the cross-talk effect, thereby enabling reliable pressure pattern measurement.

## BERGLIND ÓLAFSDÓTTIR - TOWARDS INCLUSIVE BIOMETRIC SYSTEMS

**Full Title:** Towards Inclusive Biometric Systems Assessing Face, Iris, and Fingerprint Recognition for Individuals with Congenital Disabilities
**Institution:** Technical University of Denmark
**Supervisor:** Christian Rathgeb
**Contact email:** christian.rathgeb@h-da.de

**Abstract:**
Biometric systems are a convenient and secure way to identify or verify an individual, utilising biological or behavioural characteristics. In recent years, these systems have become more widespread in various domains. With the evolution of this technology, ethical concerns have emerged regarding the inclusiveness of these systems, especially regarding minority groups. Most research today has emphasised investigating biases towards race and gender in face recognition algorithms. Unfortunately, little effort has been put into studying how inclusive biometric systems work for disabled individuals, who account for 15\% of the world’s population. This thesis aims to address the gap in knowledge and shed light on this important matter. The findings of the thesis indicate disparities in the difficulties faced by disabled individuals compared to non-disabled individuals in combination with biometric systems being significantly less utilised by disabled individuals. Furthermore, it was observed that non-disabled individuals perceive biometric systems as being more inclusive towards disabled individuals than people living with disabilities perceive them to be. The conducted usability experiment moreover confirmed that accessibility issues are a real challenge for disabled individuals when using biometric systems. The results of this thesis will hopefully encourage further research in this important research field.

## ANDERS BENSEN OTTSEN - GENERATION OF SYNTHETIC CHILDREN FACES

**Full Title:** Generative Adversarial Networks for Generation of Synthetic Children Faces
**Institution:** Technical University of Denmark (DTU)
**Supervisor:** M. Ibsen (h_da), C. Rathgeb (h_da), C. D. Jensen (DTU)
**URL:** https://dasec.h-da.de/2023/05/magnus-falkenberg-and-anders-bensen-ottsen-successfully-defended-their-master-thesis-on-generative-adversarial-networks-for-generation-of-synthetic-children-faces/
**Link description:** Completed thesis announcement
**Contact email:** mathias.ibsen@h-da.de

**Abstract:**
Biometric systems, and especially facial recognition systems, have become ubiquitous in our daily lives, serving as a reliable means of authentication for personal devices. Recently, deep learning has significantly improved the performance of facial recognition technology, albeit these approaches are dependent on the quality and quantity of the data used for training. As such, the verification performance of these systems on children is reported as subpar as there exists no large-scale unbiased database of children's faces, due to privacy concerns. However, automatic recognition of children from faces has numerous applications, including the potential to find missing or kidnapped children or analyze child sexual abuse material. Therefore, this thesis aims to address the need for a database of children's faces by using generative adversarial networks (GANs) and face age progression (FAP) models to synthesize a realistic dataset. To generate high-quality adult and corresponding child faces, the thesis performs an evaluation of various state-of-the-art FAP methods, considering several criteria, including the preservation of subject identity across ages. The final solution involves a software pipeline consisting of multiple steps and models. The pipeline initially utilizes StyleGAN3 to sample adult subjects, which are subsequently progressed to children of varying ages using InterFaceGAN, enabling direct manipulation of subjects in the StyleGAN3 latent space. Intra-subject variations, such as facial expression and pose, are created by also manipulating the subjects in their latent space. Additionally, the pipeline allows to evenly distribute the races of subjects, allowing to generate a balanced and fair dataset with respect to race distribution. Using the pipeline, a database was created, consisting of 1652 subjects and a total of 188,832 images. The significant number of images is due to each subject being present at various ages and with many different intra-subject variations. The thesis evaluates the performance of various facial recognition systems on the synthetic database and compares the results of adults and children at different ages. The study reveals that children consistently perform worse than adults, on all tested systems, and the degradation in performance is proportional to age. Additionally, the study uncovers some biases in the recognition systems, with Asian and Black subjects and females performing worse than White and Latino Hispanic subjects and males. Overall, this thesis provides valuable insights into the performance of facial recognition systems on children and highlights the need for unbiased, diverse data sets to train these systems. The synthetic database created through this work can serve as a valuable resource for researchers and practitioners in the field.

## LARS OTTERSTAD VEGGELAND - UNMASKING THE CHEATING STUDENT

**Full Title:** Unmasking the Cheating Student
**Institution:** NTNU
**Supervisor:** Patrick Bours
**Contact email:** patrick.bours@ntnu.no

**Abstract:**
Cheating in academia is as old as academia itself and is likely to always remain a thorn in its side. The emergence of computers and the internet has impacted society in countless ways, and cheating is no exception. A phenomenon known as contract cheating, where students pay someone else to write their assignments or take exams in their stead, has grown steadily in popularity among students. Such activity poses a severe threat to academic integrity, and academia is therefore in dire need of reliable methods for detecting contract cheating. Successfully identifying contract cheating is arduous since it requires an algorithm capable of handling scarce data while classifying with acceptable accuracy. This project will investigate the feasibility of the text authorship attribution technique known as unmasking to try and detect contract cheating among students. Several configurations of the unmasking algorithm will be applied to a typical authorship verification problem and assessed for viability. This project will provide an in-depth investigation of the contract cheating detection problem and whether the unmasking algorithm is a feasible solution for this problem.

## SIRI LORENZ - CONTACTLESS FINGERPRINT RECOGNITION

**Full Title:** Advanced Feature Extraction for Contactless Fingerprint Recognition
**Institution:** Hochschule Darmstadt
**Supervisor:** Christoph Busch and Jannis Priesnitz
**Contact email:** christoph.busch@h-da.de

**Abstract:**
Fingerprints have been accepted as an unchangeable, unique identifier for human identities since the 1890's and have been in use by law enforcement ever since. From that point on, fingerprint recognition has evolved and has been in operational use for decades. Most modern smartphones have finger- print capture devices and many restricted areas are protected using finger- prints as a means of identification. In recent years, especially with the spread of the COVID-19 pandemic, the need for more hygienic alternatives has gained awareness. One of those alternatives is the field of contactless fingerprint recognition. Though this field was thoroughly researched over the years, most feature extraction algorithms are still designed for the contact-based domain, with the lack of sufficient contactless training data being one of the biggest challenges. This thesis examines contactless fingerprint feature extraction. It will ex- plore two main topics: First, FingerNet, an algorithm for detecting level two features in the contact-based domain is retrained with contactless data. Hence, we present and evaluate a retraining workflow. The retrained FingerNet model was evaluated on two real world databases and compared to the original model. Second, multiple Convolutional Neural Network (CNN)s are trained to classify fingerprints based on their fingerprint patterns. We conducted 37 exhaustive experiments for classifying level one features and evaluated our trained models on three real world databases: PolyU, ISPFDv1, and hda. While retraining FingerNet leads to comparable results as the original, we show that synthetic data can be used to adapt algorithms designed for the contact-based domain to the contactless domain. Additionally, we show that CNNs trained on synthetic, contactless data are a promising method to classify fingerprint patterns, although further research is needed to improve results.

## ANŽE MUR - DEEPFAKE DETECTION

**Full Title:** Deepfake detection based on the analysis of the manipulated and non-manipulated regions
**Institution:** University of Ljubljana, Faculty of Computer and Information Science
**Supervisor:** Peter Peer, Borut Batagelj
**URL:** https://repozitorij.uni-lj.si/IzpisGradiva.php?id=150616&lang=eng
**Link description:** description and PDF
**Contact email:** peter.peer@fri.uni-lj.si

**Abstract:**
The rapid development in the field of deep learning has led to the general adoption of the deepfake concept. Deepfakes are synthetic media that are often created maliciously and therefore pose an increasingly significant challenge to modern society. For this reason, it is crucial to develop robust and effective methods for detecting deepfakes to prevent their malicious use. In our work, we implemented the Xception convolutional neural network, which we upgraded with an architecture that operates on the principle of two separate learning branches. The first branch learns only on the manipulated facial region, while the second branch uses non-manipulated regions outside of the face region to predict the final result. The implemented dual-branch architecture improves the performance of the baseline Xception model by 2.45 % in terms of AUC value from the original value of 69.76 %. We additionally trained the implemented models on a newly created synthetic dataset of deepfake artifacts, where the Xception model achieves a 12.5 % improvement in the AUC value of the baseline model with the value of 69.76 %

## MEGHANA RAO BANGALORE NARASIMHA PRASAD - FINGERPRINT MORPHING

**Full Title:** Minutiae-based Data-driven Fingerprint Morphing
**Institution:** Otto von Guericke University Magdeburg
**Supervisor:** Dr.-Ing. Andrey Makrushin, Prof. Dr.-Ing. Jana Dittman
**Contact email:** andrey.makrushin@ovgu.de

**Abstract:**
Fingerprint morphing is the process of combining two or more distinct fngerprints to create a new, morphed fngerprint that includes identity-related characteristics of all constituent fngerprints. This process can be achieved through two different approaches: A model-based minutiae-oriented approach and a data-driven Generative Adversarial Network (GAN)-based approach. The model-based approach utilizes a mathematical model to determine the location and orientation of fngerprint minutiae, whereas the data-driven approach employs Deep Neural Networks (DNNs) to produce plausible morphed fngerprints by learning from a large dataset of real fngerprints. Although the model-based approach provides the ability to manage the number of minutiae coming from the fngerprints and ensures that the morphed fngerprint biometrically matches the corresponding original fngerprints, it has a major drawback: The resulting fngerprint often appears unrealistic. On the other hand, the data-driven approach produces realistic fngerprint images. But, it does not guarantee that the resulting fngerprint matches the original fngerprints. The main objective of this thesis is to develop an algorithm that combines modelbased minutiae-oriented and data-driven GAN-based approaches to generate morphed fngerprints that look realistic and match their original fngerprints. The algorithm is developed to morph two fngerprints to generate double-identity fngerprints and is further extended to assess the feasibility of morphing three fngerprints to generate triple-identity fngerprints. The morphing process involves identifying singularities of the original fngerprints and fnding their best alignment, optimally selecting the regions of the aligned fngerprints based on the number of minutiae, encoding minutiae onto images known as minutiae maps, and fnally feeding the minutiae maps to a trained conditional GAN model, pix2pix to generate the morphed fngerprints. The results of our experiments indicate that the proposed algorithm can generate realistic double-identity fngerprints with a notable matching rate. Additionally, the results exhibit the feasibility of generating triple-identity fngerprints evaluated using the same parameters.

## ISELIN ERIKSEN ENG - CYBERGROOMING DETECTION

**Full Title:** Dynamic graph theoretical analysis of cybergrooming detection in chatrooms
**Institution:** NTNU
**Supervisor:** Patrick Bours
**Contact email:** patrick.bours@ntnu.no

**Abstract:**
The Internet has become an integral part of children's daily lives. Whether they watch YouTube videos, interact with friends on social media platforms, or engage in school activities, its presence has become inevitable. Unfortunately, the online realm also presents a concerning reality: individuals can assume any identity they desire, making it an ideal hunting ground for sexual predators. The alarming rise in reported cybergrooming cases proves there is still a need to improve measures for detecting these malicious users. In recent years, the focus has shifted not only towards detecting these predators but also towards early prevention strategies, to prevent them from causing trauma to the children. Throughout this thesis, we have investigated the possibilities of detecting predators and other users displaying inappropriate behaviour by studying simulations of the individual user's behaviour over time. Further, we have implemented supervised \gls{ml} algorithms as a way to classify how their behaviour changed throughout the monitored time-frame. With this implemented, we created a detection mechanism which aims to balance identifying their behaviour as soon as possible and achieving high precision and recall. From our results, we concluded that detecting \textit{abnormal} users (for example; sexual predators, spammers, scammers and users involved in sexting) early by monitoring their dynamic behavioural chat patterns in ongoing conversations is possible. In the future, it would be interesting to investigate further ways to improve the earliness of the detection, whilst maintaining precision and recall, by looking at fine-tuning parameters and identifying potential initial-stage behavioural patterns. The possibility of designing a mechanism which combines early-detection approaches should also be investigated to see if this would enhance the early detection performance.

## CORNELIA VEDELD PLESNER - SOFT BIOMETRICS IN DISTORTED KEYSTROKE DYNAMICS DATA

**Full Title:** Privacy vs. Security: Soft Biometrics in Distorted Keystroke Dynamics Data
**Institution:** NTNU
**Supervisor:** Patrick Bours
**Contact email:** patrick.bours@ntnu.no

**Abstract:**
In today's rapidly evolving digital landscape, the preservation of privacy and security can be a daunting task. Utilizing keystroke dynamics to enhance authentication and identification techniques is a promising approach that increases security, but at the same time raises important privacy considerations to address. Hence, this thesis aims to investigate whether distortion of Keystroke Dynamics data can hinder the detection of soft biometric characteristics, such as age and gender. A program was used to simulate and add distortion to the data in combination with the Google plug-in tool "Keyboard Privacy". The data underwent processing and subsequent analysis using the Machine Learning model Support Vector Machine in order to classify age and gender. Additional analysis was carried out to determine if it was possible to detect any distortions within the dataset. The study revealed that there are distinguishable differences between distorted and non-distorted keystroke dynamics data. While the patterns may bear similarities, they are still distinct enough to enable relatively accurate classification. The performance of the distorted dataset may vary depending on the classification categories, where gender classification performed better than age classification. These findings shed a light on the possibility of developing more sophisticated systems for biometric identification and authentication.

## VENKATA SRINATH MANNAM - SECURING GENERATOR OF A GAN

**Full Title:** Securing Generator of a GAN by training with watermarked images
**Institution:** Otto-von-Guericke University Magdeburg
**Supervisor:** Dr.-Ing. Andrey Makrushin, Prof. Dr.-Ing. Jana Dittman
**Contact email:** andrey.makrushin@ovgu.de

**Abstract:**
With the rapid growth of generative adversarial networks (GAN) and the resulting increase in the production of high volumes of robust deepfakes. It is crucial to identify and prevent their malicious use. The term ”deepfakes” refers to synthetic media that involves replacing a person with someone else in an existing video or image. Our media is fngerprints and same kind of image manipulation is caused by the GANs. Deepfakes are often of such high quality that neither human nor automated detection approaches can easily identify them as fake. While deepfakes have useful applications in certain domains, they can also be used maliciously, posing a threat to security systems. Unique noises or patterns produced by deepfakes, and watermarking training data(by another neural network) have been used to identify them. We propose a novel approach to secure the GAN model by training it with watermark-embedded data using digital image processing techniques. Our study investigates the transferability of watermarks using a state-of-the-art Conditional-GAN(CGAN) model, popularly known as pix2pix, trained with watermarked fngerprints data. We explore two hybrid watermarking algorithms based on discrete cosine transformation (DCT), discrete wavelet transformation (DWT), and singular value decomposition (SVD). The results show that the CGAN learns the watermarking distribution, resulting in excellent watermark recovery rates, with one watermarking algorithm outperforming the other watermarking algorithm. We optimize performance by varying the watermarking parameters, and the GAN parameters. Future research can explore other watermarking techniques, extend the idea to other forms of media such as audio or video, and training with different GAN models, to enhance the robustness of the process.

## RICARDO CORREIA - EXPLAINABLE FACE RECOGNITION USING VISION TRANSFORMERS

**Full Title:** Explainable Face Recognition using Vision Transformers
**Institution:** Instituto Superior Tecnico - Universidade de Lisboa, Portugal
**Supervisor:** Paulo Lobato Correia and Fernando Pereira
**URL:** https://fenix.tecnico.ulisboa.pt/cursos/meec21/dissertacao/565303595503744
**Link description:** Explainable Face Recognition using Vision Transformers
**Contact email:** paulo.lobato.correia@tecnico.ulisboa.pt

**Abstract:**
This M.Sc. thesis is dedicated to advancing the transparency of face recognition (FR) models employed for face verification (FV) tasks, with a special emphasis on the promising Visual Transformers (ViTs). ViTs have gained prominence as a valuable tool for FR, due to their self-attention mechanism, which can be explored to improve the explainability of FV decisions. To achieve this objective, the thesis introduces a novel methodology for generating FV explainability heatmaps, designed to explain any type of FV decisions. This approach leverages the attention maps generated by ViTs post-hoc tools and employs masking techniques to highlight salient regions within these attention maps. The masking technique with the biggest impact on the FV process is utilized to generate heatmaps, shedding light on the pivotal facial regions influencing the verification outcome. Furthermore, the thesis proposes a novel FV model and a novel XFR tool that adopts a hybrid approach, integrating both ante-hoc and post-hoc methods to explain FV decisions. The ante-hoc approach involves the incorporation of multiple ViTs, one of which is dedicated to learning a global face representation, while others, the face landmarks ViTs, specialize in distinct facial regions. This use of LViTs enhances the transparency of the FV process, as the embeddings generated by each LViT are associated with specific facial landmarks, enabling the generation of ante-hoc explainability heatmaps. Additionally, a post-hoc approach generates FV explainability heatmaps by combining the produced ViT post-hoc tools attention maps from the FV decision pair.

## JAKUB REŠ - TESTING THE ROBUSTNESS OF A VOICE BIOMETRICS SYSTEM AGAINST DEEPFAKES

**Full Title:** Testing the Robustness of a Voice Biometrics System against Deepfakes
**Institution:** Brno University of Technology
**Supervisor:** Kamil Malinka
**URL:** https://www.vut.cz/en/students/final-thesis/detail/144004
**Contact email:** iresj@fit.vut.cz

**Abstract:**
Topic of this paper is a methodology of testing the robustness of a voice biometric system against deepfakes. The main problem currently lies in insufficient coverage of testing against the presentation attack using deepfakes in ISO/IEC standards. The aim of this thesis is to cover the hole, resulting from emergence of deepfake technology, by proposing an extended methodology, based on the existing one, that focuses on fixing the issue. The solution of proposed problem started by studying the state of the art for deepfakes and standard practices of biometric system testing. Second, I proposed and documented a method of testing the voice biometric system. The test was designed as a scenario, where the Phonexia voice biometric system is used as a remote verification tool for the voice-as-a-password use-case. For the purpose of demonstration, the online publicly available dataset was used. On top of test design, I set a non-standard metric for the test evaluation to show possibilities of focus on different kinds of deepfakes. After carrying out tests and evaluating results, I formulated the procedure into a generic repeatable methodology, containing practices and recommendations. The contribution of this work lies in incorporating deepfakes into the existing standard methodologies of testing a biometric systems, hence forming and demonstrating a repeatable methodology.

## PERNILLE KOPPERUD - BIAS MITIGATION IN FACE RECOGNITION

**Full Title:** Bias Mitigation in Face Recognition Systems using Synthetic Data
**Institution:** Norwegian University of Science and Technology
**Supervisor:** Christoph Busch and Marcel Grimmer
**URL:** https://github.com/pernilko/MSc_FR_Bias
**Link description:** Official Repository
**Contact email:** marceg@ntnu.no

**Abstract:**
Today, most modern face recognition systems are based on deep learning techniques that require a large amount of labelled training data in order to perform adequately. With the introduction of privacy laws and regulations, such as the GDPR, it has become increasingly difficult to collect large and diverse datasets of face images sufficient to train well-performing face recognition systems. Consequently, the use of synthetic data to train face recognition systems has gained attention. This is because synthetic data has the potential to both alleviate the privacy issues faced when collecting real-world data and offer greater control over the data used to train face recognition systems. In this thesis, the use of synthetic data to train face recognition systems is explored. Specifically, the thesis aims to explore if it is possible to build an unbiased synthetic dataset that can be used to fine-tune existing face recognition systems to reduce bias with respect to age. Further, the thesis aims to investigate how the use of synthetic face images affects the performance of face recognition systems. The results show that there exists a prominent domain gap between synthetic and real face images that causes the performance of face recognition systems fine-tuned on synthetic data to generalize poorly to real-world data. Introducing real face images to the synthetic training dataset can help close the domain gap and boost the performance of the system. Furthermore, the results show that using an unbiased synthetic dataset has the potential to reduce bias with respect to age if the domain gap is closed.

## OLIVER DAGSLAND TVERRÅ - CONTINUOUS DETERMINATION OF AGE AND GENDER

**Full Title:** Continuous Determination of Age and Gender
**Institution:** NTNU
**Supervisor:** Patrick Bours / Estelle Cherrier
**Contact email:** patrick.bours@ntnu.no

**Abstract:**
When someone communicates online with another person, there are many aspects that is not known in regards to these parties. The individuals that communicate may also have malicious intentions, and as a result may lie in regards to age and gender. As a result of this, a victim of such intent can suffer consequences like inappropriate pictures being shared online, grooming attempts or physical harm. By utilizing keystroke dynamics, it is possible to determine a human's age or gender. Some studies have achieved varying results in this regard by utilizing keystroke dynamics and communication data. In this study, the determination of age and gender will be the focus; the age and gender groups was divided into 2 classes respectively. However, in a continuous manner, using keystroke dynamics that results in the continuous determination of soft biometrics with keystroke dynamics. The output will be further analyzed, processed and then represented statistically. Research in the area displays promising results when basing the prediction on the full data set and periodic predictions. The earliest determination of gender with satisfactory accuracy achieved for this study was a mean of 126 keystrokes and an accuracy of 71%. The highest accuracy was 87.5% with 1644 keystrokes. For age the earliest was a mean of 312 keystrokes with 72\% accuracy, the highest accuracy was 77% with 825 mean keystrokes. There were approximately 1750 keystrokes for each participant, meaning that the earliest determination needed approximately 7% of the participant's writing to determine gender and 17% of the writing in terms of age. Therefore, it is found that it is possible to determine gender and age continuously and early but at the cost of accuracy.

# YANNIK SCHÄFER - IMPROVING DEMOGRAPHIC FAIRNESS FOR FACE RECOGNITION

**Full Title:** Improving Demographic Fairness for Biometric Face Recognition Systems
**Institution:** Hochschule Darmstadt
**Supervisor:** Christoph Busch, Jascha Kolberg
**Contact email:** christoph.busch@h-da.de

**Abstract:**
With the rise of deep neural networks, the performance of biometric systems has increased tremendously. Biometric systems for facial recognition are now used in everyday life. The systems are used among other things for entry control at borders, crime prevention, or private device access control. Although the accuracy of these systems is generally high, they are not without flaws. Biometric systems in many cases have a demographic bias. Different demographic groups are therefore not recognized equally well. This is especially true for facial recognition, among other things, due to the demographic features of gender and skin color being clearly visible in images of human faces. This thesis investigates if well-chosen model combinations for decision- and/or score-level fusions can improve the fairness of the fused models in the verification scenario. For this purpose, twelve different models of four different face recognition algorithms were evaluated. The baseline parameter for all models is an FMR of 0.1%.The models used for fusion were determined based on three selection criteria: the models with the lowest False-Match-Rate FMR for an individual demographic group, the three fairest models for a covariate, and the pareto-efficient models for FMR-Fairness and False-Non-Match-Rate FNMR. The fusions were evaluated by FMR-Fairness, FNMR, and individual group-specific FMR. It was found that it is possible to improve the fairness between specific demographic groups in single cases and make the fusion model fairer than the initial models. In twelve out of 33 fusions, the fairness of the initial models was improved by a fusion. Different types of mergers have different influences on performance parameters. A general statement that fusion can improve the fairness and/or accuracy of biometric systems cannot be made. But some trends are recognizable: The best selection criterion was the lowest FMR for an individual demographic group. The fusions were most successful in improving fairness between gender and skin color but did only in two cases improve the fairness between subgroups of those. The fusions with only two models were always fairer than the initial models, this was not the case with fusions of three models. The Or-fusion was the only fusion that alleviated the bias between subgroups.

# MONITOR
# BACHELOR-THESES

## JORGE DE MIGUEL PIRES - ANALYSIS OF BEHAVIORAL BIOMETRICS USING MOBILE DEVICES

**Full Title:** Analysis of behavioral biometrics using mobile devices
**Institution:** Universidad Autonoma de Madrid
**Supervisor:** Ruben Vera Rodriguez
**URL:** https://repositorio.uam.es/handle/10486/700637
**Link description:** UAM repository
**Contact email:** ruben.vera@uam.es

**Abstract:**
Information stored in our cell phones is becoming more and more abundant and sensitive. That is why we must keep it protected and prevent any unauthorized access to it. Nowadays, there are several security measures to prevent this type of intrusions, but most of them only allow us to keep the device locked while it is not being used. In this thesis we will study a security measure that is currently being developed. This method consists of continuous user authentication based on behavioral biometrics from data collected by the device's sensors. This new measure allows us to identify in a continuous and non-intrusive manner if the person using the device is the owner of it. This way, if the user is detected not to be the owner, the device is automatically locked to prevent unwanted access to the information. Throughout this work, we will try to solve a doubt regarding this type of systems. This doubt consists of clarifying whether there is a bias introduced due to sensor differences and calibration imperfections across devices that the system is using to recognize the user. The presence of this bias would be a problem in this method of authentication, since it would make it easier for an intruder to trick the system. To investigate this possible problem, we will use mathematical tools such as Fourier Transforms to analyze whether there are noise frequencies from the sensors of the device present in the data that could be influencing the decisions of the system. In addition, we will implement deep learning models to try to classify the data according to the device from which they come, thus checking if, in case there is a sensor bias in the data, it is enough for a model to learn patterns from it and distinguish between different device models.

## LAVRA ŠTRUMBELJ - COMPARATIVE ASSESSMENT OF FACIAL LANDMARKING TECHNIQUES

**Full Title:** Comparative assessment of facial landmarking techniques
**Institution:** University of Ljubljana, Slovenia
**Supervisor:** Vitomir Štruc
**URL:** https://repozitorij.uni-lj.si/Dokument.php?id=173785&lang=slv
**Link description:** The PDF is available for the thesis - in Slovene
**Contact email:** vitomir.struc@fe.uni-lj.si

**Abstract:**
Human identification is getting ubiquitous in our everyday lives, where algorithms verify identities based on various physical and behavioural attributes. This thesis is focusing on one step in this process, that is detecting facial landmarks, which is usually the first step in the identification process, on several image databases. Specifically, it compares three detection models, which are based on computer vision. Those are Supervised Descent Method or SDM, Tasks-constrained deep convolutional network or TCDCN for short and Multi-Center Network, also called MCNet. The goal of the thesis is to understand how these methods behave under varying circumstances, how image and facial characteristics influence their success and to determine their respective advantages and disadvantages. Firstly, we lay the foundation with an overview of existing research, that provides a broader view of the state of the profession. In the theoretical part is then presented the basic theoretical background of detecting facial landmarks and the chosen methods for their detection that will be evaluated. The section on the methodology of the work describes the image databases used in the experiments and the methodology for evaluating the results. Installation and implementation of the methods and the tools used are also described in depth. As part of the thesis, 5 experiments were carried out, which focused on the verification of methods for certain categories of images according to gender, race and proximity of persons, as well as according to the importance of the colour information of the images and the conditions they were captured under. Lastly, the results and the problems encountered by the methods in detecting facial landmarks were presented, as well as general observations and findings of the thesis. The achieved results are briefly summarised and suggestions for further research are given.

## VALENTINA FOHR - EVALUATION OF FUSION METHODS FOR MULTI-BIOMETRIC CRYPTOSYSTEMS

**Full Title:** Evaluation of Fusion Methods for Multi-Biometric Cryptosystems
**Institution:** Hochschule Darmstadt
**Supervisor:** Christian Rathgeb
**Contact email:** christian.rathgeb@h-da.de

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

## BARTOSZ KOZLOWSKI - IMAGE QUALITY ASSESSMENT IN IRIS RECOGNITION

**Full Title:** Ocular image quality assessment for the purposes of iris recognition
**Institution:** Wroclaw University of Science and Technology
**Supervisor:** Wojciech Wodo
**URL:** https://github.com/Kozlowski-Bartosz/Iris-image-quality-assessment
**Link description:** Github repository
**Contact email:** kozlowski.bartosz@protonmail.com

**Abstract:**
Iris recognition is one of the most efficient methods of biometric verification. The performance of an iris recognition system is, however, heavily affected by the quality of biometric data provided to the system. The quality of iris images is often reduced by imperfect measurement conditions, the user's unfamiliarity with the system's operating procedures, or other external factors. This thesis describes the design and implementation of a system that would allow for determining the quality of iris images supplied to the biometric system based on the quality metrics described in the ISO/IEC 29794-6:2015 international standard. The work consists of four chapters. Chapter 1 explains general concepts related to iris processing in a biometric systems. Chapter 2 presents the ISO/IEC 29794-6:2015 standard and describes ten basic quality measures that were implemented in the designed application. Chapter 3 describes the tools used and the structure of said system. The final chapter, chapter 4 contains an in-depth description of the project's implementation.

## FABIO NOTARO - FEDERATED LEARNING FOR MORPHING ATTACK DETECTION

**Full Title:** Federated Learning for Morphing Attack Detection
**Institution:** University of Bologna
**Supervisor:** Annalisa Franco
**Contact email:** annalisa.franco@unibo.it

**Abstract:**
The problem addressed in this thesis is Face Morphing Detection, i.e., the recognition of altered and counterfeit facial images in order to enhance and strengthen today's biometric security systems, found for example in airports. The solution explored is Federated Learning, a branch of Deep Learning more focused on privacy and data protection, which may represent one of the few approaches that can comply with today's stringent regulations on the protection of sensitive data. In particular, the thesis, after a detailed explanation of the morphing problem and analysis of the potential benefits of Federated Learning, explores the use of the NVFlare framework, a product developed by NVIDIA that enables the training of machine learning models through, precisely, the use of Federated Learning. At the end of the thesis, conclusions and considerations are drawn about the work done and the results obtained.

## DANIEL PRUDKÝ - ASSESSING THE HUMAN ABILITY TO RECOGNIZE SYNTHETIC SPEECH

**Full Title:** Assessing the Human Ability to Recognize Synthetic Speech
**Institution:** Brno University of Technology
**Supervisor:** Anton Firc
**URL:** https://www.vut.cz/en/students/final-thesis/detail/140541
**Contact email:** ifirc@fit.vut.cz

**Abstract:**
This work responds to the development of artificial intelligence and its potential misuse in the field of cybersecurity. It aims to test and evaluate the human ability to recognize a subset of synthetic speech, called voice deepfake. This paper describes an experiment in which we communicated with respondents using voice messages. We presented the respondents with a cover story about testing the user-friendliness of voice messages while secretly sending them a pre-prepared deepfake recording during the conversation and looked at things like their reactions, their knowledge of deepfakes, or how many respondents correctly identified which message was manipulated. The results of the work showed that none of the respondents reacted in any way to the fraudulent deepfake message and only one retrospectively admitted to noticing something specific. On the other hand, a voicemail message that contained a deepfake was correctly identified by 96.8% of respondents after the experiment. Thus, the results show that although the deepfake recording was clearly identifiable among others, no one reacted to it. And so the whole thesis says that the human ability to recognize voice deepfakes is not at a level we can trust. It is very difficult for people to distinguish between real and fake voices, especially if they are not expecting them.

## BINE MARKELJ - CREATING FAKE VIDEOS USING DIFFUSION MODELS

**Full Title:** Creating fake videos using diffusion models to expand the dataset for fake video detection
**Institution:** University of Ljubljana, Faculty of Computer and Information Science
**Supervisor:** Peter Peer, Borut Batagelj
**URL:** https://repozitorij.uni-lj.si/IzpisGradiva.php?id=149326&lang=eng
**Link description:** description and PDF
**Contact email:** peter.peer@fri.uni-lj.si

**Abstract:**
In the bachelor's thesis we present techniques and procedures for generating deepfake videos. These are videos that were subjected to manipulations with deeplearning techniques. In our thesis we specialized on the topic of deepfakes, where the facial area was manipulated. They are usually made with the help of special generative adversarial networks - GAN. Such videos represent a major problem in the spread of fake news, political propaganda, destruction of individual's public image, production of pornographic content, extortion, etc. In the thesis we describe in detail different types of fake videos from deepfake database FaceForensics++. We also present our own method for potential creation of a subset of the mentioned database using the latest generative diffusion models. These models progressively generate images (or videos) from latent noise. We use a specific open source diffusion model called stable diffusion, that is used for generating images from text and image prompts. We describe multiple techniques, that we used and tested in our experiment and analyze their quality and success. We also comment on the utility and danger posed by fake videos generated by diffusion models.

## DAVIDE CELLOT - FACE MORPHING AND MORPHING ATTACK DETECTION

**Full Title:** Face Morphing and Morphing Attack Detection
**Institution:** University of Bologna
**Supervisor:** Annalisa Franco
**Contact email:** annalisa.franco@unibo.it

**Abstract:**
Biometric facial recognition systems are now found in many areas of daily life. They are used to identify people, find images of the same person in a collection of digital images, to make suggestions for tagging people on social media, or for verification tasks such as unlocking a phone or computer. Beyond these consumer market applications, biometric facial recognition systems have also found their way into sovereign tasks such as automated airport border control. In particular, for these tasks, the verification system must be reliable and secure. In recent years, in the area of face recognition, it has been noticed how it is possible to create an artificial image of a face, by means of other known face images, so similar to them that it is very complex to distinguish the real from the fake. This specific security attack is called Face Morphing Attack. Morphing Attack Detection is still an open area of research because there is no algorithm that can determine with 100% accuracy whether an image is real or has been altered. In the Thesis, special attention will be given to the case of Automated Border Controls, automated airport gates that use facial recognition to verify a passenger's identity and either allow or deny them access to the country. And it will conclude that the topic of Morphing Attack Detection is still open and security not yet as comprehensive as it should be. The research is continuing its work, confident that there will be more developed technologies to counter criminals in the future.

## ANDRII FEDUNIV - SPRECHERVERIFIKATION ALS TEIL EINER MULTIFAKTOR-AUTHENTIFIZIERUNG

**Full Title:** Sprecherverifikation als Teil einer Multifaktor-Authentifizierung
**Institution:** Hochschule Darmstadt
**Supervisor:** Jascha Kolberg
**Contact email:** christoph.busch@h-da.de

**Abstract:**
These days, many companies offer their customers the convenience of handling various tasks remotely, including through the use of the voice channel. With just one phone call, customers can make a bank transfer or inquire about their health insurance coverage. To make this possible, the customer's identity must first be verified, which can be done using traditional methods such as passwords or tokens, as well as through multifactor authentication. This study focuses on the use of speaker verification as a component of multifactor authentication, while taking into account the current ISO standard for usability and security in biometrics. The study proposes methods for enrolling, identifying, and verifying speakers. In addition, the study examines how the context and length of spoken phrases during the enrollment of speaker profiles can impact verification results. The study also aims to strike a balance between security and user convenience in authentication. The study tests and verifies both genuine users and impostor attempts to gain access using various datasets. Finally, the study selects a practical solution for registering and verifying speakers using spoken digit strings. With the help of Google's Speaker ID, the study achieves a secure and successful verification of authentic speakers, with no false non-match rate. Although the false match rate during intrusion attempts is 7%, it is considered acceptable since an additional passphrase increases the overall security in this multi-factor authentication.