Biometric Systems - Research Projects

email: christoph.busch (at) h-da.de

Copenhagen, June 2, 2022

1 DTU Course 02238

The research project is an essential part of the course. Each student is expected to select a topic, conduct the research project and to summarize the results in a term paper. The term paper must define the problem or research project area, clearly explain the current state of the art where appropriate and the relative merits of the principal approach (and implementation) covered.

While guidance for literature will be provided, a partial objective of graduate studies is to acquaint students with graduate research in the primary literature. Hence, students are expected to independently identify relevant literature from primary and secondary sources during the composition of their term paper.

Suggested topics are described in this document. The topics are quite different in nature: Some require more theoretical work, some are experimental and others require good implementation skills. However all of them address current research challenges in the field of Biometrics ranging from presentation attack detection to biometric sample quality assessment. These topics are to be researched and analyzed by students on an individual basis. Select from the list of topics or develop your own topic. If you propose a complementary topic you need to get approval for that via email (see contact details above).

1.1 Teaching Assistant

Please address any question regarding the topics or regarding the starting material to the teaching assistants Mathias Ibsen and Pia Bauspiess. To get the quickest possible response, consider putting both teaching assistants as a recipient on any emails. Before you write an email, kindly check if your question has been answered in the FAQ at the end of this document.
Email: mathias.ibsen (at) h-da.de
Email: pia.bauspiess (at) ntnu.no

2 Schedule for Research Assignments

Schedule

Date	Event
June 2, 2022	Research topics for term papers provided
June 07-10, 2022	Lectures
June 09, 2022	Final registration for research topic
June 11-23, 2022	Individual work on research topic
June 27, 2022	Submission of research report

3 Submission of Research Result

The result of your research will include a term paper and a data zip-file.

3.1 Term Paper

The term paper should be a 12 page document that would be suitable for submission to a scientific conference. All term papers should be formatted using the LaTeX typesetting system in the format used for the Lecture Notes on Informatics (LNI).
Word-template:
https://biosig.de/fileadmin/TG/BIOSIG/BIOSIG2022/LNI-Word-Template_en_final.doc
LaTeX-template:
https://biosig.de/fileadmin/TG/BIOSIG/BIOSIG2022/LNI-LaTeX-Template_en_final.zip

The use of biometric terms in your paper must be compliant with the International Standard ISO/IEC 2382-37 Biometric Harmonized Vocabulary. In consequence replace for instance any occurrence of the term *matching* with *comparison* and use the term *template* only in a context, where you actually refer to a set of extracted biometric features. The standardized terms and definitions are provided at:
http://www.christoph-busch.de/standards.html
The biometric performance evaluation must be reported in accordance with ISO/IEC IS 19795-1 Biometric performance testing and reporting. A script for producing DET-curves will be provided.

The paper should report about your achievements. You should choose an appropriate structure for the report and include references to all material that you have used.

- The filename of the term paper should be 02238-xxxxxxx-yyy.pdf (where xxxxxxx is your student id and yyy is the topic three letter acronym as given later in this document)
- The term paper should be uploaded to the DTU learn (`https://learn.inside.dtu.dk`) on June 27, 2022 (no later then 23.59h). Note that we can not negotiate extensions to this deadline, which is already some days after the official ending of the course.

3.2 Zip-File

For most term papers topics it will be appropriate to submit additional data that relates to your term paper (e.g. source code or articles that you have referenced). In that case you should submit a zip-file containing all data files that are of relevance for your term paper and also containing a README.txt describing the content.

- The filename of the zip-file should be 02238-xxxxxxx-yyy.zip
- Upload the zip-file to the DTU-learn:
  `https://learn.inside.dtu.dk`

3.3 Individual Work

The research conducted in this course is by definition an individual project. Therefore the generation of an individual report is mandatory. Any one project topic can be chosen by at most five students.

3.4 Evaluation

The assessment of your research results will respect a number of criteria that you should consider, when selecting the appropriate research topic. The criteria include the following aspects:

- Quality of the achievements
- Quality of the report and documentation
- Extent of material that was provided for this topic
- Level of innovation
- Amount of work that was required (e.g. implementations)
- Difficulty of the task – indicated in parentheses in the header of every topic description later on in this document. The difficulties range from 0.0 to 1.0 (higher is more difficult).

The term paper shall not repeat content from the lecture. Moreover late submission of the term paper will be penalized without regard to the actual merit of the paper or submission. This penalty will apply except in case of documented emergency (e.g. in case of medical emergency), or by prior arrangement at the discretion of the instructor. All written work submitted must carry the student's name and must be reasonably neat and well organized. Any work that cannot easily be read will be penalized.

3.4.1 Academic Integrity

Penalties will particularly be imposed for academic dishonesty. Academic dishonesty is defined as any action or practice that provides the potential for an unfair advantage.

Academic dishonesty includes the misrepresentation of facts, the fabrication or manipulation of data or results, representing another's work or knowledge as one's own, disrupting or destroying the work of others, or abetting anyone who engages in such practices.

Academic dishonesty is not absolute because the expectations for collaboration vary. However, unless given specific permission, any and all results submitted must be the result of individual effort, performed without the help of other individuals or outside sources.

You are kindly reminded on DTU's regulations on plagiarism at exams as follows: *"DTU considers it cheating if an examinee submits work that is not a result of his or her own independent merit or if prohibited aids are utilized at an examination. Similarly, DTU considers it cheating for any student to assist another student in breaching the examination rules. Examples of cheating at examinations include copying the work of others, copying own answers from previous examinations and any communication concerning examination questions during individual, supervised examinations. Written assignments may be presented for assessment once only. Assignments previously assessed at DTU or other academic institutions may not be submitted for renewed assessment irrespective of the grade earned. The rules regarding citations and references to sources in written assignments are that citations must be indicated by quotation marks at the start and at the end of the citation and the source of the citation must be referred to either in brackets or in a note to the text. When not citing directly but basing the discussion on a specific source, the source must be referred to either in brachets or a note to the text."*

If a question arises about the type of external materials that may be used or the amount of collaboration that is permitted for a given task, each individual involved is responsible for verifying the rules with the instructor or teaching assistants before engaging in collaborative activities, using external materials, or accepting help from others.

4 Research Topics

The following research topics are provided. They will be presented in the first lecture. The topics have different difficulty levels ranging from 0.0 to 1.0 (higher is more difficult), such that harder work will be rewarded. The full range of grades are achievable with all topics, however. Detailed discussions on the topics are possible in the breaks between the lectures or at the end of each teaching day. You may also come up with your own topic idea, but note that a *prior* written approval (via email) of such topic by the course instructor is *mandatory*. At all times you can address questions regarding the research project to the course instructor or teaching assistants via email. Before you do so, check if your question is already answered in the FAQ section at the end of this document. For every email question, please refer to the research topic via the three letter acronym (topic-id) that is indicated for each topic in the title of the following subsections.

Note on Survey Topics

Several of the provided research topics are surveys. These topics consist of literature research and a report on the reviewed papers. The value of a survey is *structuring*, *comparing* and *systematizing* a large number of research contributions to a given topic (typically between 100-200). Due to the shorter time available in this course, a lower number of 20-50 papers is sufficient. Note that a survey does not include describing in detail how you found the papers (e.g., how many hits you got on Google Scholar), and also does not include copying or rephrasing the abstract of every paper found. Instead, systematic work on the literature should be performed, which is the only way to receive a good grade on a survey topic in this course. Good examples of surveys in the area of biometrics are:

- M. Grimmer, R. Raghavendra, and C. Busch: Deep face age progression: A survey. IEEE Access, 2021
- P. Drozdowski, C. Rathgeb, and C. Busch: Computational workload in biometric identification systems: An overview. IET Biometrics, 2019
- T. Schlett et al.: Face image quality assessment: A literature survey. ACM Computing Surveys (CSUR), 2021

4.1 Machine Learning for Fingerprint Recognition: An Overview (MFR)(0.4)

Provide an overview of machine learning methods for biometric fingerprint recognition.

4.1.1 Background

Machine learning methods have received a huge amount of attention in the last years. They are also increasingly used in the field of biometric fingerprint recognition and implement various tasks throughout the recognition pipeline (e.g. capturing, enhancement, quality assessment, feature extraction, comparison).

4.1.2 Task

The task is to:

- Present an overview on the most important machine learning methods for different stages of the recognition pipeline. Where possible, compare the methods empirically in accordance with ISO/IEC 19795-1.
- Discuss advantages and drawbacks of machine learning methods in comparison to non-learning approaches.

4.1.3 Expected Outcome

- Overview paper (with bibliography) of proposed methods.
- Discussion of advantages and drawbacks.

4.1.4 Starting Reading and other Material

- Tang, Yao, et al. FingerNet: An unified deep network for fingerprint minutiae extraction. 2017 IEEE International Joint Conference on Biometrics (IJCB), 2017.
- ISO/IEC 19795-1

4.2 Contactless Fingerprint Feature Extraction and Comparison (FPE)(0.9)

Evaluate an existing feature extraction and comparison algorithm on contactless fingerprint databases.

4.2.1 Background

The VeriFinger Fingerprint feature extraction and comparison algorithm shows a good performance on samples captured using different types of capturing devices. This project evaluates its performance on contactless fingerprint images.

4.2.2 Task

Evaluate the performance of VeriFinger on a given database.

4.2.3 Expected Outcome

- Install the given software.
- Perform the feature extraction and comparison.
- Report the biometric performance as given in ISO/IEC 19795-1

4.2.4 Reading and other Material

- Malhotra et al.: Fingerphoto Authentication Using Smartphone Camera Captured Under Varying Environmental Conditions
- Priesnitz et al.: An overview of touchless 2D fingerprint recognition
- Preprocessed contactless fingerprint database
- Verifinger SDK
- DET script
- ISO/IEC 19795-1

4.3 Modeling realistic 2D contactless Finger Images (MTL)(0.7)

Synthetically generated biometric data has to be as realistic as possible to be beneficial for biometric systems developing.

4.3.1 Background

With SynCoLFinGer we proposed a first method for the generation of synthetic contactless finger images based on Python and OpenCV. However, the produced contactless fingerprint images are not looking very realistic.

4.3.2 Task

The task is to improve existing layers (e.g. generation of wounds) and/or implement new layers (e.g. dermatological issues) to make the fingerprint image more realistic.

- Improve the visual resemblance of an existing layer which models wounds
- Add new modelling layers like rotation, water drops or dermatological influences to the algorithm
- Find suitable parameters to control the variance for each layer
- Discuss the filters you implemented and how they compare to the already existing filters. Furthermore, discuss potential improvements

4.3.3 Expected Outcome

- New or improved modelling layers (integrated in the software)
- Report including detailed description of the method

4.3.4 Starting Reading and other Material

- Priesnitz et al. SynCoLFinGer: Synthetic Contactless Fingerprint Generator. arXiv preprint arXiv:2110.09144.
- SynCoLFinGer project

4.4 Color-based Comparison of contactless Fingerprint Images (CCF)(0.7)

Implement and evaluate a comparison algorithm for contactless fingerprints which is based on the color of the fingertip.

4.4.1 Background

Apart from minutiae, contactless fingerprint images contain more features which could improve the recognition accuracy. The skin color could be one of them.

4.4.2 Task

The task is to implement a color based comparison algorithm.

- Compute the average color of pre-segmented fingerprint images
- Implement a comparison algorithm
- Report your recognition accuracy according to ISO/IEC 19795-1

4.4.3 Expected Outcome

- Preprocessing and comparison algorithm
- Report including detailed description of the performance

4.4.4 Starting Reading and other Material

- ISO/IEC 19795-1
- ISPFDv2 database (pre-segmented)
- DET script

4.5 Survey on Hand Recognition (SHR)(0.4)

A comprehensive survey on available hand and contactless palm- and hand-recognition systems together with databases used for this purpose.

4.5.1 Background

There is limited work addressing hand recognition in forensic scenarios where a part of the hand might only be visible to systems (e.g. back of the hand, palm, etc.). There is also a limited number of databases for this purpose. Therefore, covering the above two points can contribute to the development of new hand recognition systems.

4.5.2 Task

Conduct a survey on research that include:

- Hand recognition and Contactless Palmprint recognition systems. Specify which of them are open-source systems. Include information on the techniques used for hand recognition.
- Available databases. For each database, specify characteristics such as visible parts of the hands (i.e., dorsal, palm, etc). Are images taken in unconstrained scenarios?
- Report biometric performance of available systems according to ISO/IEC 19795-1, where the reviewed literature adheres to it

4.5.3 Expected Outcome

- Survey with Bibliography of reviewed works.

4.5.4 Starting Reading and other Material

- W. M. Matkowski, T. Chai, A. W. K. Kong,. Palmprint recognition in uncontrolled and uncooperative environment. In IEEE Trans. on Information Forensics and Security, 15, 1601-1615, 2019.
- V. Kanhangad, A. Kumar, D. Zhang,. A unified framework for contactless hand verification. IEEE Trans. on information forensics and security, 6(3), 1014-1027, 2011.
- ISO/IEC 19795-1

4.6 Face Morphing Attack Detection (MAD)(0.8)

Implement a method for detecting morphed face images.

4.6.1 Background

A criminal can create a facial morph that can bypass an automated face recognition system by using image morphing and morphing his/her own face with that of an accomplice. Detecting such morphed images is of paramount importance.

4.6.2 Task

- Implement a method for single or differential morphing attack detection (you can also use an existing pre-trained model if you can find one)
- Benchmark the method, in accordance with ISO-standards, on a provided database of morphed and bona fide images.
- Compare your results with other results reported in the literature

4.6.3 Expected Outcome

- An evaluation according to ISO/IEC IS 30107-1 of (at least) one morphing attack detection algorithm on a dataset of bona fide and morphed face images
- An brief overview of methods for morphing attack detection and comparison of the proposed method with other methods in the literature

4.6.4 Starting Reading and other Material

- Bona fide and morphed images from the FERET and FRGCv2 datasets
- M. Ferrara, A. Franco, and D. Maltoni: The magic passport. in IEEE International Joint Conference on Biometrics (IJCB), 2014.
- R Raghavendra, K. Raja, C. Busch. Detecting Morphed Face Images. In 8th IEEE International Conference on Biometrics: Theory, Applications, and Systems, 2016.
- ISO/IEC IS 30107-1,
- DET script

4.7 Survey on Child Face Recognition (SCR)(0.4)

A comprehensive survey on available children recognition systems together with databases used for this purpose.

4.7.1 Background

Robust face recognition for children (including ageing impact) is an open area of research. Research on this topic tends to use databases that are not publicly available or only contain images of specific demographic groups, e.g. very young children (newborns) from India. The few public databases that include children's faces tend to be from only a few subjects and are usually compiled from public footage, e.g. television series.

4.7.2 Task

Conduct a survey on those studies that include:

- Face recognition system for children. Specify which of them are open-source systems. Info on the techniques used for this purpose.
- Available databases. For each database specify characteristics such as age ranges, ethnic group, etc.
- Report biometric performance of available systems.

4.7.3 Expected Outcome

- Survey with Bibliography of reviewed works.

4.7.4 Starting Reading and other Material

- S. L. M. Oo and A. N. Oo,. Child Face Recognition with Deep Learning, in Proc. Intl. Conf. on Advanced Information Technologies (ICAIT), pp. 155-160, doi: 10.1109/AITC.2019.8921152, 2019.
- D. Deb, N. Nain, A. K. Jain,. Longitudinal study of child face recognition, in Proc. Intl. Conf. on Biometrics (ICB) (pp. 225-232). IEEE. 2018.
- K. Bahmani and S. Schuckers,. Face Recognition In Children: A Longitudinal Study. arXiv preprint arXiv:2204.01760, 2022.

4.8 Face Mask Analysis (FMA)(0.7)

Analysis of the impact of face masks on the performance of a face recognition system.

4.8.1 Background

When face recognition systems are employed in unconstrained application scenarios (e.g., for surveillance), some faces might be partially occluded by masks. This study shall investigate the impact of masked face images on a face recognition system.

4.8.2 Task

- Describe state-of-the-art for handling masked faces in the context of face recognition systems
- Create an appropriate database of masked face images (by adding masks to the given images). The database should also contain ground-truth images without masks
- Use existing face recognition algorithms and measure the impact of face masks, i.e. by comparing the performance of the masked faces to the performance of the ground-truth images without masks. Include into your evaluation the impact of masks on face detection
- Report the results using appropriate ISO/IEC standards

4.8.3 Expected Outcome

- Description of approaches for handling masked faces in face recognition systems
- A database of masked and ground-truth face images
- A performance benchmark investigating the impact of face masks on (at least) one open-source face recognition system

4.8.4 Starting Reading and other Material

- Subset of FERET or FRGCv2 face database, code to generate DET-curves, ISO/IEC-19795-1 standard
- ArcFace (`https://github.com/deepinsight/insightface`) or other state-of-the-art open-source face recognition systems
- MaskTheFace (`https://github.com/aqeelanwar/MaskTheFace`) or other open-source algorithms for adding masks to faces. You can also make your own mask designs!

4.9 Tattoo Detection Survey (DTS) (0.4)

Conduct a survey on methods for detecting and recognizing real tattoos.

4.9.1 Background

Many individuals get tattoos on different parts of their body, often for aesthetic or descriptive purposes but they have historically also been used for various functional purposes such as identification. Detecting and recognizing tattoos can help police agencies identify individuals, but it can also be used for other purposes such as automated (digital) tattoo removal.

4.9.2 Task

- Conduct a survey on methods for tattoo detection and recognition
- Discuss why tattoo detection and recognition might be of interest and which (if any) ethical issues there might be with using tattoos for person identification

4.9.3 Expected Outcome

- A comprehensive survey on methods for tattoo detection and recognition

4.9.4 Starting Reading and other Material

- https://www.nist.gov/programs-projects/tattoo-recognition-technology
- Ibsen et al. “Face Beneath the Ink: Synthetic Data and Tattoo Removal with Application to Face Recognition”: (https://arxiv.org/abs/2202.05297)
- Hrkać et. al, "Deep learning architectures for tattoo detection and de-identification," First Int’l Workshop on Sensing, Processing and Learning for Intelligent Machines (SPLINE), 2016

4.10 Face Morphing Capacity (FMC)(0.8)

Explore the capacity of morphed face images.

4.10.1 Background

Some countries offer web-portals for passport renewal, where citizens can upload their face photo. These applications allow the possibility of the photo being altered to beautify the appearance of the data subject or being morphed to conceal the applicants identity. Specifically, if an eMRTD passport is issued with a morphed facial image, two or more data subjects, likely the known applicant and one or more unknown companion(s), can use such passport to pass a border control. It has been shown that up to 4 subject faces can use one passport.

4.10.2 Task

- Investigate the capacity of morphed face images: How many data subjects could use one single passport?
- Select a suitable morphing tool (e.g. FantaMorph, GIMP-GAP)
- Generate morphed facial images (from 2 subjects) and confirm that both subjects can be recognized with their probe image.
- Generate morphed facial images from 3,4,5, ... subject and repeat in each step the recognition validation
- Report the capacity of the morphed images under constraint of recognition. Report the capacity difference, when you morph with random partners versus lookalikes (e.g. same gender, same age, same skin-color)

4.10.3 Expected Outcome

- A comprehensive report on the challenges of morphing and the technical details of numerous data subject potentially using one single passport.

4.10.4 Starting Reading and other Material

- subset of FERET and FEI database
- ArcFace (open source face recognition tool)
- M. Ferrara et al. The magic passport IJCB 2014
- M. Gomez-Barrero et al. "Is Your Biometric System Robust to Morphing Attacks?", IWBF 2017.
- U. Scherhag et al. "Biometric Systems under Morphing Attacks: Assessment of Morphing Techniques and Vulnerability Reporting", BIOSIG 2017
- ISO/IEC IS 30107-1 and ISO/IEC IS 30107-3

4.11 Face Beauty Score (FBS)(0.4)

Investigate methods and metrics to assess the beauty of a facial image.

4.11.1 Background

It is a well known fact that human experts can better recognize faces from celebrities that those from unknown normal individuals. When it comes to morphing attacks, some psychologists claim that the averaging of two faces lead to a more beautiful face. Thus if one would have a measure for beauty, one could potentially derive a method for detecting morphed face images.

4.11.2 Task

Conduct a survey on currently available methods for measuring the attractiveness of facial images. Include a comprehensive overview of existing open-source software in the area and evaluate the usefulness of such implementations

- Investigate the literature from psychology, medicine and pattern recognition for such methods
- Summarize the approaches found and differentiate between real beauty and perceived beauty. It is recommended that you illustrate the measures for a small set of images.

4.11.3 Expected Outcome

- A comprehensive state-of-the-art survey (with bibliography) of methods and existing open-source software for measuring the beauty of facial images
- Discussion of capabilities, and strengths and weaknesses of the surveyed approaches

4.11.4 Starting Reading and other Material

- Ramon et al. Familiarity matters: A review on prioritized processing of personally familiar faces
- Jones et al. Does facial attractiveness really signal immunocompetence?
- Eulerich et al. Do Fine Feathers Make a Fine Bird? The Influence of Attractiveness on Fraud-Risk Judgements by Internal Auditors
- Beholder-GAN https://github.com/beholdergan/Beholder-GAN

4.12 Blurred Face Image Quality (FIQ)(0.8)

Investigate metrics that measure the quality of blurred facial images.

4.12.1 Background

Biometric systems can only perform well if the reference data and the probe data is of sufficient sample quality. Thus it is of high importance to control the quality of facial images, before they are stored in a reference database.

4.12.2 Task

Analyze the ISO/IEC 29794-1 (framework), ISO/IEC 29794-5 (face) and ISO/IEC 29794-6 (iris) and investigate how well the suggested metrics predict the blurriness/sharpness of (face) images.
Suggested methodology: 1) Create progressively blurrier versions of a set of presumably sharp initial face images. 2) Implement a selection of the suggested blur-related quality metrics. You can also use existing implementations where available, specifically SHARPNESS from the 29794-6 standard. 3) Analyze the correlation between the quality scores and the known blur strengths for the images.
Optional task extension: Compute comparison scores for mated face image pairs for each blur strength, to show how the comparison scores are affected by the blur.

4.12.3 Expected outcome

- Blurred image variants based on a set of provided face images.
- Implementations of selected face blur quality metrics
- Graphs showing statistics (e.g. the mean) for the computed quality scores across the image variants
- Analysis of the correlation between quality scores and the known blur strengths for each face blur quality metric.

4.12.4 Starting Reading and other Material

- ISO/IEC 29794-1,5,6.
- Face images from ColorFERET.
- ArcFace (open source face recognition tool).
- Python face image quality assessment framework
- P. Grother: Performance of Biometric Quality Measures, IEEE, 2007.

4.13 Face Anonymisation Experiments (FAE)(0.8)

4.13.1 Background

In recent years, privacy has arisen as a major concern associated with biometric systems. Obscuring or anonymising faces in images and videos is one option, which can be used to protect privacy, while retaining certain level of visual coherence/intelligibility of the image. Various techniques, including blurring, covering eyes, etc. exist for this purpose. In this project, their efficacy will be evaluated experimentally.

4.13.2 Task

Conduct experiments with currently available methods for anonymisation of facial images. Create a database of faces with varying strength of anonymisation and evaluate the biometric performance on those, as well as the unaltered images.

4.13.3 Expected Outcome

- Implement own or use existing open-source methods for facial image anonymisation
- Use the methods to create a database of images with varying degrees of face obfuscation/anonymisation (e.g. filter to the whole facial region or eyes only, various levels of the filter intensity etc.)
- Apply open-source biometric recognition to evaluate the effects of the used anonymisation methods. In particular, report the results using DET curves, as well as the percentages of face detection failures.
- Write a report describing your experimental setup, the created database, and the results, along with a discussion thereof

4.13.4 Starting Reading and other Material

- Ruchaud and Dugelay: "Automatic Face Anonymization in Visual Data: Are we really well protected?"
- Ren et al.: "Learning to Anonymize Faces for Privacy Preserving Action Detection"
- ArcFace (https://github.com/deepinsight/insightface)
- Subset of the FERET facial image database
- DET curve software

4.14 Face Stretching Analysis (FSA)(0.7)

Face recognition is a very popular biometric approach, which reaches good biometric performance metrics.

4.14.1 Background

Facial images are stored in passports and used at border control to authenticate the passport holder. Unfortunately some individuals stretch the facial images, before printing it. The study shall investigate the impact of stretched images on a face recognition system.

4.14.2 Task

- Conduct an extensive literature survey and analyze the current state of the art with respect to approaches to handle stretched faces in the context of face recognition.
- Use an existing face database and generate a stretched database with controlled stretching parameters (from mild to severe) in both horizontal and vertical direction.
- Use an existing face recognition algorithm and measure the impact of stretching (from no stretching to severe).
- Report your results using the metrics specified in the ISO/IEC standard and compare your own results with the results from your literature survey.

4.14.3 Expected Outcome

- Report on the current algorithmic approaches to handle stretching in the area of face recognition and a performance evaluation on generated database.

4.14.4 Starting Reading and other Material

- Subset of face images from the FERET and FRGCv2 database
- ArcFace (https://github.com/deepinsight/insightface)
- ISO/IEC-19795-1
- DET curve software

4.15 Survey about Face Age Modification (SAM)(0.4)

Survey the latest progress on using deep learning for face age progression.

4.15.1 Background

Face recognition systems have to be robust against intra-identity variations. In particular, performance limitations due to face ageing are challenging to measure since the collection over long time spans is time-consuming and expensive. To overcome the lack of available data, face age progression techniques are employed to simulate the human face ageing process. The generated age-modified face images are then used to evaluate/increase the robustness of existing face recognition systems. This work aims to summarise the latest progress in face age modification.

4.15.2 Task

- Research state-of-the-art face age modification techniques.
- If code available: Compare ageing results on a small dataset (will be provided)
- Write a survey by summarising the main concepts and open challenges.

4.15.3 Expected Outcome

- A list of state-of-the-art face age modification techniques.
- Few ageing examples comparing the results of different face age modification works.
- A comprehensively-written and well-structured survey.

4.15.4

- Grimmer et al., Deep face age progression: A survey, IEEE Access, 2021.
- Wu et al., Adversarial UV-Transformation Texture Estimation for 3D Face Aging, IEEE Access, 2021.
- Li et al., Continuous Face Aging via Self-estimated Residual Age Embedding, CVPR, 2021.

4.16 Survey about Face Age Estimation (SAE)(0.4)

Survey the latest progress on using deep learning for face age estimation.

4.16.1 Background

Face recognition systems have to be robust against intra-identity variations. In particular, performance limitations due to face ageing are challenging to measure since the collection over long time spans is time-consuming and expensive. To evaluate the ageing accuracy of face age progression methods, age estimation is used to predict the ground-truth age labels. This work aims to summarise the latest progress in face age estimation.

4.16.2 Task

- Research state-of-the-art face age esimation techniques.
- Focus on works with publicly available codes.
- Evaluate and compare the age estimation performance on a small (self-collected) database
- Write a survey by summarising the main concepts and open challenges.

4.16.3 Expected Outcome

- A list of state-of-the-art face age estimation techniques.
- A performance comparison of the age estimators based on a self-collected database.
- A comprehensively-written and well-structured survey.

4.16.4

- Grimmer et al., Deep face age progression: A survey, IEEE Access, 2021.
- Zhang et al., C3AE: Exploring the limits of compact model for age estimation, stability, and variation, IEEE Access, 2018.
- Zeng et al., Soft-ranking label encoding for robust facial age estimation, IEEE Access, 2020.

4.17 Survey about Head Pose Estimation (SPE)(0.4)

Survey the latest progress on using deep learning for head pose estimation.

4.17.1 Background

The performance of biometric recognition systems often depends on single factors of variations, such as age, illumination, or facial expression. In particular, head pose differences between the reference and probe sample can deteriorate the recognition accuracy significantly. It is still challenging to evaluate the performance drop with varying head poses due to the lack of available samples annoted with the exact rotation angles. To solve this issue, head pose estimation techniques are used to predict the ground-truth pose rotations, enabling a more precise testing of face recognition systems. This work aims to summarise the latest progress in head pose estimation.

4.17.2 Task

- Research state-of-the-art head pose esimation techniques.
- Focus on works with publicly available codes.
- Evaluate and compare the pose estimation performance on a small (self-collected) database
- Write a survey by summarising the main concepts and open challenges.

4.17.3 Expected Outcome

- A list of state-of-the-art head pose estimation techniques.
- A performance comparison of the pose estimators based on a self-collected database.
- A comprehensively-written and well-structured survey.

4.17.4

- Albiero et al., img2pose: Face Alignment and Detection via 6DoF, Face Pose Estimation, CVPR, 2020.
- Hempel et al., 6D Rotation Representation For Unconstrained Head Pose Estimation, ICIP, 2022.

4.18 Face Recognition Evaluation using Face Compensation Illumination (DCE)(0.8)

Use a pre-trained deep learning compensation illumination method to improve the performance on a database which contains poor conditions and shadows on faces. The goal is to analyse the influence of the pre-trained illumination compensation method on face recognition performance.

4.18.1 Background

Illumination changes are widespread in real life capturing scenarios, for instance, in a face verification system applied at an automated border control (ABC) gate. In this scenario, real-life face images present shadows on different face areas, making the face recognition process difficult. This project aims to study the influence of illumination compensation on face images and evaluate the performances in face recognition systems to improve the recognition task. Illumination compensation method and database will be provided.

4.18.2 Task

- Evaluate baseline database on a face recognition system
- Create a new version of baseline database using pre-trained compensation illumination methods
- Evaluate the influence of the illumination methods on the face recognition system
- Develop a report with appropriate metrics (ISO-compliant)

4.18.3 Expected Outcome

- Introduction and short description of methods
- Overview and Interpretation of the experimental results
- Report with DET curves and metrics

4.18.4 Starting Reading and other Material

- Guo et. al, "Zero-reference deep curve estimation for low-light image enhancement", CVPR, 2020
- Chongyi et. al, "Learning to Enhance Low-Light Image via Zero-Reference Deep Curve Estimation", TPAMI, 2021
- ZeroDCE and Zero DCE++Compensation method: https://li-chongyi.github.io/Proj_Zero-DCE.html
- Face-recognition System: https://github.com/serengil/deepface
- ISO/IEC 19795-1 standard and face database

4.19 Data Projection on Morphing Images (DPM)(0.7)

Use a no-linear data projection tool t-SNE map to analyse the clusterization of bona fide and morphed face images.

4.19.1 Background

A t-SNE map projection is used to visualise how the data is projected to a 2D plot. This method shows non-linear connections in the data. The t-SNE algorithm calculates a similarity measure between pairs of instances in the high dimensional and low dimensional spaces. It then tries to optimise these two similarity measures using a cost function. The goal is to apply and analyse the projection of bona fide and morphed images created with different morphing tools. The two databases and t-SNE methods will be provided.

4.19.2 Task

- Evaluate default projection on morphing database.
- Analyse how the different morphing methods and post-processing of the provided database affect the projection.
- Evaluate how changing the parameters of the t-SNE affect the results.
- Develop a report with metrics.

4.19.3 Expected Outcome

- Introduction, motivation and short description of methods.
- Overview and Interpretation of the experimental results.
- Report with metrics.
- Deliver python files.

4.19.4 Starting Reading and other Material

- Visualisation of High Dimensional Data using tSNE - An Overview https://jmlr.csail.mit.edu/papers/volume9/vandermaaten08a/vandermaaten08a.pdf
- t-SNE implementation: https://github.com/shivanichander/tSNE
- Face database

4.20 Face recognition evaluation using Super-Resolution (SSR)(0.7)

Use a pre-trained super-resolution method to evaluate the influence of super resolution on a face recognition system.

4.20.1 Background

Super-resolution (SR) is the process of recovering a high-resolution (HR) image from a low-resolution (LR) one. In this scenario, real-life face images present artefacts in the background and illumination changes in some relevant face areas that make it difficult to recognise the faces. This project aims to study the influence of SR on face recognition performance and improve eventually the face recognition system accuracy. Pre-trained super-resolution methods and database will be provided.

4.20.2 Task

- Evaluate baseline database (without SR) on a face recognition system
- Create new version of baseline database on pre-trained super-resolution methods x2 and x3 and x4
- Evaluate influence of super resolution on a face recognition system
- Develop a report with DET curve and relevant metrics.

4.20.3 Expected Outcome

- Introduction and short description of methods
- Overview and Interpretation of the experimental results
- Report with DET curves and metrics (ISO compliant)

4.20.4 Starting Reading and other Material

- Tapia et. al, "An Efficient Super-Resolution Single Image Network using Sharpness Loss Metrics for Iris," 2020 IEEE International Workshop on Information Forensics and Security (WIFS), 2020, pp. 1-6, doi: 10.1109/WIFS49906.2020.9360886.
- Lim et. al, "Enhanced Deep Residual Networks for Single Image Super-Resolution," 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), 2017, pp. 1132-1140, doi: 10.1109/CVPRW.2017.151.
- Super-resolution Implementations: https://github.com/krasserm/super-resolution
- Face-recognition System https://github.com/serengil/deepface
- Face database

4.21 Analysing Explainable Visualisation for Morphing Attack Detection (AEV)(1.0)

Use the Layer-wise Relevance Propagation (LRP) algorithm to visualise the classifier's prediction for a morphing detection problem.

4.21.1 Background

The visualisation of features used for the Deep Learning (DL) method is an open problem. DL methods are considered black-box models, therefore visualisation i.e., explainability is necessary for a better understanding on the DL method. Layer-wise Relevance Propagation (LRP) is a method that identifies relevant pixels by running a backward pass in the neural network. The backwards pass is a conservative relevance redistribution procedure, where neurons that contribute the most to the higher layer receive the most relevance from it. This project aims to visualise the most relevant features on morphed face image classifiers using deep learning.

4.21.2 Task

- Train a simple DL classifier to detect morphed images.
- Implement a visualization of the most relevant features on the images.
- Develop graphics and visualization for several examples (morphing methods).
- Evaluate Average-pooling and Max-pooling stages.
- Analyse the consistency of the results (Does the features selected make sense?)

4.21.3 Expected Outcome

- Introduction and short description of methods
- Overview and Interpretation of the experimental results
- Visualization from morphed images (database provided)
- Report with DET curves and metrics

4.21.4 Starting Reading and other Material

- LRP: https://www.jmlr.org/papers/volume17/15-618/15-618.pdf
- U. Scherhag, C. Rathgeb, J. Merkle and C. Busch, "Deep Face Representations for Differential Morphing Attack Detection," in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 3625-3639, 2020, doi: 10.1109/TIFS.2020.2994750.
- Single Morphing Attack Detection using Feature Selection and Visualisation based on Mutual Information (https://arxiv.org/pdf/2110.13552.pdf)
- https://github.com/sebastian-lapuschkin/lrp_toolbox

4.22 Survey on Detection of Digital Face Manipulations (DFM)(0.4)

A comprehensive survey of approaches for digital face manipulation detection and how these can improve the security of face recognition systems.

4.22.1 Background

Digital face manipulations are any alterations to a face which occur in the digital domain, examples include face swapping, morphing, and retouching. Researchers have shown that manipulated faces can impair the efficacy of face recognition systems. To mitigate this, researchers are currently developing approaches for detecting digitally manipulated face images.

4.22.2 Task

Conduct a survey on existing methods for detecting digital face manipulations. Motivate the work by describing how digital face manipulations can hamper face recognition performance and lead to loss of trust in digital content. Describe different approaches by answering the questions:

- Which detection algorithm is used?
- What kind of manipulations are considered?
- How is the algorithm trained and how well does it compare to other approaches?
- Is there any freely available implementation of the method?
- Discuss advantages and disadvantages of the different approaches as well as current research challenges

4.22.3 Expected Outcome

- Survey (with Bibliography) of the reviewed approaches.

4.22.4 Starting Reading and other Material

- Rathgeb et al., Differential Detection of Facial Retouching: A Multi-Biometric Approach, 2020
- Ferrara et al., The magic passport, 2014
- Ibsen et al., Differential Anomaly Detection for Facial Images, 2021
- Scherhag et al., Face Recognition Systems Under Morphing Attacks: A Survey, 2019

4.23 Free 2D Face Recognition Software (FRS)(0.4)

Analysis of free 2D face recognition software

4.23.1 Background

Facial recognition software is the basis for intelligent video surveillance systems. Today there are not only commercial solutions available. Some free software solutions are available.

4.23.2 Task

- Perform an investigation on open source 2D face recognition software libraries and software development kits. Briefly describe at least three SDKs and explain your decisions for or against a specific SDK
- Implement a face recognition system using at least one of the SDKs you found.
- Evaluate the performance of the SDK and report you results with the metrics from the ISO/IEC 19795-1 standard.
- Point out the virtues and limitations of you face recognition algorithm by looking at false matches and false non-matches. Try to explain these errors.
- Compare the recognition performance of the SDKs with DET curves.

4.23.3 Expected Outcome

- Report on open source (2D) face recognition software libraries / SDKs and the algorithm used
- Implementation of an example in programming language of choice
- Report on biometric performance benchmark

4.23.4 Starting Reading and other Material

- http://www.face-rec.org
- ISO/IEC-19795-1
- Code to generate DET curves
- Subsets of face images from FERET and FRGCv2

4.24 Benchmarking Facial Soft-Biometric Extractors (BFE)(0.7)

Find and benchmark open-source software for extraction of soft-biometrics from facial images.

4.24.1 Background

Soft-biometric features (for example, sex, ethnicity, age, eye colour etc.) can be extracted from facial images. They can be used, for instance, in order to enhance the biometric performance of a primary recognition system or for indexing large-scale biometric databases.

4.24.2 Task

- Find open-source software for extraction of soft-biometrics from facial images
- Groundtruth for some traits may have to be created by the student (you)
- Perform tests and report/compare the accuracy of the software against each other and the ground-truth
- Discuss open problems and future research perspectives in the area

4.24.3 Expected Outcome

A report containing (but not necessarily limited to):

- An description of state-of-the-art methods for estimating the chosen soft-biometric features
- A benchmark and comparative assessment of the tested approaches

4.24.4 Starting Reading and other Material

The following items can serve as a starting point for investigations on this topic:

- IMDB-Wiki dataset with partial groundtruth
  `https://data.vision.ee.ethz.ch/cvl/rrothe/imdb-wiki/`
- A. Dantcheva *et. al.* What Else Does Your Biometric Data Reveal? A Survey on Soft Biometrics
- Handbook of Face Recognition
- ISO/IEC 19795-1

4.25 Post-Quantum Secure Biometric Systems (PQB)(0.4)

Conduct a literature survey on the current state-of-the-art in post-quantum protection for biometric systems.

4.25.1 Background

Biometric data are sensitive personal data that require long-term protection. Therefore, post-quantum cryptography (PQC) is considered in an increasing amount of works for the protection of biometric systems. However, PQC is a relatively new field of research itself. Therefore, no established approaches to biometric template protection in the quantum age exist yet. The goal of this paper is to find out in what different ways biometric systems are secured against attacks using quantum computers (independent of biometric modalities). A broad and comprehensive literature review is more important than a detailed description of the different approaches. A particular point of interest are the assumed threat models (i.e., security against passive or active quantum adversaries) and the arguments made for the post-quantum protection of biometric data.

4.25.2 Task

- Review literature on post-quantum secure biometric systems (breadth rather than depth)
- List the threat model each approach operates under
- Provide a short comparison of the approaches

4.25.3 Expected Outcome

- Comprehensive literature survey on post-quantum secure biometric systems
- Comparison of the surveyed papers, in particular i.t.o. threat models

4.25.4 Starting Reading and other Material

- J. Kolberg et al, Efficiency analysis of post-quantum-secure face template protection schemes based on homomorphic encryption, 2020
- P. Bauspiess et al. Post-Quantum Secure Two-Party Computation for Iris Biometric Template Protection, WIFS 2020.
- R. Arjona et al., A Post-Quantum Biometric Template Protection Scheme Based on Learning Parity With Noise (LPN) Commitments, 2020

4.26 Survey on Inclusive Fairness in Biometrics (IFB)(0.4)

The usage of biometric systems assumes that the majority of subjects is in a good health condition to actually use the system. But how many people are excluded from using those systems?

4.26.1 Background

Fingerprint recognition does only work if you have fingers. The same holds for other biometric modalities. Face recognition systems mostly orientate themselves by aligning both eyes. What happens if a subject has only one eye, or none? Do some health conditions have side-effects, which limit the usage of biometrics?

4.26.2 Task

The task is

- Screen literature and internet for health statistics worldwide/EU/USA/some specific country
- Discuss which influence those health issues could have on using biometrics
- Discuss whether those biometrics can be named fair in terms of inclusion

4.26.3 Expected Outcome

- Report on health statistics and biometrics
- References for the statistics you present

4.26.4 Starting Reading and other Material

- World Health Organisation https://www.who.int/
- Amputee-Coalition. "Limb Loss in the USA." Inside Track, 01/04/2016, 3.
- https://www.statista.com/topics/4274/global-health/

4.27 Early-Decision for Biometric Identification (EDI)(0.7)

Evaluate the performance of early-decision in biometric face identification systems.

4.27.1 Background

A significant challenge in large-scale biometric identification is its computational efficiency. The most expensive operation in such a system is the computation of the comparison function of two templates, as the number of comparisons grows linearly with the size of the enrolment database. For biometric modalities that can be represented in ordered templates like face, iris, and fingerprint, a promising idea is therefore to skip the computation of scores that will be rejected. E.g., if a distance function is used for the comparison, the computation can be aborted once the score is higher than a previously computed score.

4.27.2 Task

- Run baseline open-set biometric identification, starting with face (code available in C++ and Python)
- Determine suitable block sizes for the comparison of two templates
- Evaluate the computational and biometric performance of aborting the computation of the comparison scores after they exceed the previous minimal score

4.27.3 Expected Outcome

- Evaluation of computational and biometric performance of early-decision approach for face identification
- Argumentation about chosen block sizes
- Overview and interpretation of the experimental results

4.27.4 Starting Reading and other Material

- P. Drozdowski et al., Computational workload in biometric identification systems: an overview, IET Biometrics 2019.
- J. Kolberg et al., Template protection based on homomorphic encryption, WIFS 2019
- Face templates from FRGC database
- Code for baseline biometric identification

4.28 Own Project Topic (OPT)(1.0)

You can propose your own topic for the term paper. Note, that a **prior** written (via email) approval of the proposed topic by the course instructor is **mandatory**. The proposed topic should follow the same format as the ones provided in this document.

5 Topic assignments

Once you have carefully considered and chosen your research topic you can register your topic on the following website
https://framadate.org/F6FFMwASiiebT2wF
Password: Bio22DTU
Please write your full name in the name field when registering. Each topic can be chosen by up to five students. Note that the first come - first served principle is applied.

6 Starting Material

For most research topics there is a set of starting material available: The material will be handed to you during the first week via download link. Before you can get the data - please print, sign and scan the NDA contained at the end of this document. Once we receive an email with your signed NDA, you will get in return the access information.

Note that the material is partly protected under copyright regulations and is provided for your PERSONAL academic use only. Redistribution of the material in any way is prohibited. Further note, that the provided material is meant merely as a starting point for your project. In your work, you will be required to identify additional relevant materials and literature from primary and secondary sources yourself.

7 NDA: Software/Data Use and Non-Disclosure Agreement

Please submit this form to the teaching assistants (see first page of this document).

I am participating in the Course Biometric Systems (02238). I acknowledge that software / sensitive biometric data provided by the instructor Christoph Busch and/or the teaching assistants in this course is provided for use in this course only. The software / biometric data will be used for the research project conducted in the course only. Any use after completion of the course is not permitted.

I do declare that I will treat the software/data in a confidential manner and that I will delete any copy within a week after completion of the 02238 course.

Any test results obtained during the usage of the software under this course agreement will not be published nor disclosed to third parties without written agreement of the instructor.

Mandatory information:

ThreeLetterAcronym of the course topic: ______________________________

Name: ____

Lyngby, date, signature: ____

8 Frequently Asked Questions

In this section we answer the following questions:

- How do I register for a term paper topic?
- Do I have to submit exactly 12 pages?
- How should I format my report?
- Do I have to use the starting material provided for my term paper topic?
- How do I find the difficulty of my topic and what does it mean?
- I am trying to use a face recognition system, but it takes a lot of time to do comparisons. What can I do?
- My topic is a survey topic. How should I approach it?
- How do I evaluate the performance of a biometric system?
- How do I obtain the starting material for my topic?
- I have problems installing the necessary dependencies to run a repository. What can I do?
- How should I hand in my term paper?
- How to propose my own term paper topic?

You are of course welcome to approach the teaching assistants via email at any time if you have additional questions.

How do I register for a term paper topic?

Once you have carefully considered and chosen your research topic you can register your topic on the following website
https://framadate.org/F6FFMwASiiebT2wF
Password: Bio22DTU
Please write your full name in the name field when registering. Each topic can be chosen by up to five students. Note that the first come - first served principle is applied.

Do I have to submit exactly 12 pages?

No, 11-13 pages are okay, but please stay within these page limitations. Writing an overly long or short paper is likely to affect the grade of the term paper.

How should I format my report?

Please use the LaTeX or Word template specified in section 3.1 of this document. You are allowed to make minor changes to the template, but please do not change anything that might affect the report's length, such as text size, margin, spacing, etc.

Do I have to use the starting material provided for my term paper topic?

The starting material is meant to help you write your paper, and in most cases, you should use the starting material and find new material on your own. Some topics ask that you use specific algorithms or software, in which case you should try to do this; other topics are more generic and, for instance, ask you to evaluate how specific actions affect a biometric system. In such cases, you are free to choose other algorithms than the ones listed, but you should, where possible, try to use at least one state-of-the-art system.

How do I find the difficulty of my topic and what does it mean?

The difficulty of your topic is given as a numerical value in the title of your term paper topic. For instance, for the topic "Modeling realistic 2D contactless Finger Images (MTL)(0.7)", the topic acronym is MTL, and the difficulty is 0.7. The difficulty is given on a scale from 0 to 1, where 1 means more difficult. The difficulty of the topic will be taken into consideration during the grading; however, despite the difficulty of your topic, it is possible to achieve both the lowest and highest grade.

I am trying to use a face recognition system, but it takes a lot of time to do comparisons. What can I do?

There are several things you can try to do to speed up the computations of any face recognition system. The first step is to use the GPU if your pc has a GPU which supports CUDA. Another thing is to make sure that you only extract the feature embeddings once per image. A typical mistake is not to reuse the feature embeddings when during the non-mated comparisons. Therefore, make sure that you first extract the feature embeddings from all your images and save them to your disk or in-memory in a data structure with a fast look-up time, e.g. a dictionary.

My topic is a survey topic. How should I approach it?

Start by reviewing the lecture content relevant to your topic. This should give you the basics to understand the research papers you will be reading. Make sure that you have a clear understanding of what your survey topic is and what new insights it should provide to a reader. Afterwards you can start on finding recent research papers on the topic by using search tools such as Google Scholar, IEEE Xplore or the ACM Digital Library. These websites also link papers that the paper you are looking at references, or which works reference the paper you are looking at, both of which can be relevant. Note that this list is not comprehensive and that you should find your own strategy to find all relevant research papers for your survey. You can use tools like Zotero or similar to keep track of the literature you find.

The idea behind a survey is structuring, comparing and systematizing a large number of research contributions to a given topic (typically between 100-200). Due to the shorter time available in this course, a lower number of 20-50 papers is sufficient. Note that a survey does not include describing in detail how you found the papers (e.g., how many hits you got on Google Scholar), and also does not include copying or rephrasing the abstract of every paper found. Instead, systematic work on the literature should be performed, which is the only way to receive a good grade on a survey topic in this course. If you want to take a look at good examples of recent surveys in the area of biometrics, consider:

- M. Grimmer, R. Ramachandra, and C. Busch: Deep face age progression: A survey. IEEE Access, 2021
- P. Drozdowski, C. Rathgeb, and C. Busch: Computational workload in biometric identification systems: An overview. IET Biometrics, 2019
- T. Schlett et al.: Face image quality assessment: A literature survey. ACM Computing Surveys (CSUR), 2021

How do I evaluate the performance of a biometric system?

We have created a tutorial which will be presented on 09.06.2022 at 08.00h. The Jupyter notebook for the tutorial is available to students who have signed and returned the NDA to one of the teaching assistants. The notebook can be found in the script folder and is called "DET-tutorial-python". The tutorial focus on biometric verification, which is sufficient for most term papers, but similar principles can be applied for biometric identification. Additionally, students working with biometric performance evaluation should consult ISO/IEC 19795-1. For students working with presentation attacks or morphing attacks, ISO/IEC IS 30107-1 should be consulted.

How do I obtain the starting material for my topic?

Fill out and sign the NDA in section 7 of this document and send it to the teaching assistants. After that, you will be given download links which contain the starting material for your topic. Research papers are not distributed but should be available as open-access or through DTU Findit.

I have problems installing the necessary dependencies to run a repository. What can I do?

Try installing all the dependencies in an isolated environment, for instance, using Conda (if you are working with python). Be sure to read the installation instructions of the repository and be observant about any prerequisites of your system; for instance, the Bob signalling toolkit from Idiap only works on Linux and macOS 64-bit operating systems. If the problem persists and you have been unable to resolve the issue using online sources, contact the teaching assistants. Try to describe the problem as concise as possible and preferably include a description of how to reproduce the errors you get.

How should I hand in my term paper?

The term paper should be uploaded to DTU learn `https://learn.inside.dtu.dk` and follow the naming convention described in section 3.1 of this document. Additionally, you are asked to upload all additional data used to reproduce your paper's results, for instance, code and generated images. The additional data should be bundled into a Zip file and named as described in section 3.2 of this document. You should include a README file which describes the content of the zip. It is unnecessary to upload any of the data provided by us as starting material; however, data derived from this, for instance, new images, should be uploaded. In case you exceed the memory limitations of DTU Learn, you can include a download link and password on DTU learn to where the additional data can be downloaded from. It is **very important** that if you upload the data to any external services such as a cloud provider that you encrypt the zip before uploading it. In this case, you should also add the password for decrypting the content of the zip as a comment to DTU learn.

How to propose my own term paper topic?

You are welcome to propose your own term paper topic. Find a topic that interests you and which is related to biometric systems. Then, approach the course instructor or one of the teaching assistants to discuss the topic. If we think the topic is good, you are asked to write a one-page description of the term paper topic following the same format as the term paper topics provided in this document. After that, the document should be submitted to the course instructor. Note that written approval by the course instructor is **mandatory**.