Biometric Systems - Research Projects

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

Copenhagen, June 1, 2023

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 01, 2023	Research topics for term papers provided
June 06-09, 2023	Lectures
June 09, 2023	Final registration for research topic
June 12-23, 2023	Individual work on research topic
June 27, 2023	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/BIOSIG2023/LNI-Word-Template_en_final.doc
LaTeX-template:
https://biosig.de/fileadmin/TG/BIOSIG/BIOSIG2023/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 in a scientific writing and presentation style. You should choose an appropriate structure for the report and include references to all material that you have used. A list with helpful suggestions on academic writing is included at the end of this document. Please note that the term

paper shall not repeat lecture content, but build on top of the lecture content and highlight your own research contribution.

- 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, 2023 (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 generated data). 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, but the topics are not meant as group projects.

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. This also applies to text, images, results, or any material generated by external tools such as using Chat-GPT or similar.

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 literature 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. Generally speaking, a good starting point to a survey topic can be to construct a taxonomy (which will be part of your research contribution) of reviewed approaches in the style of Fig. 2 in: Drozdowski et al., "Computational workload in biometric identification systems: An overview", IET Biometrics, 2019, and to analyze and compare the reviewed works accordingly.

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)

Conduct a systematic overview (survey) on 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:

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

4.1.3 Expected Outcome

- Survey paper 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 Fusion of Contactless Fingerprint PAD algorithms (FCF)(0.7)

This paper will investigate approaches for fusing the scores of different algorithms for contactless fingerprint presentation attacks detection (PAD).

4.2.1 Background

Methods for recognizing individuals based on contactless fingerprints have become popular in recent years due to their convenience and increased hygiene compared to contact-based fingerprint recognition. However, such algorithms can be spoofed using various presentation attack instruments such as silicone fingers. To prevent this, different methods for detecting contactless fingerprint presentation attacks have been proposed. For this topic, you will receive a list of scores from different PAD algorithms. Scores of PAD algorithms can be fused in order to achieve a better detection of presentation attacks. The task is to implement fusion strategies for contactless fingerprint PAD algorithms in order to improve the detection accuracy.

4.2.2 Task

- Research approaches for performing fusion of fingerprint PAD scores
- Given PAD scores from different algorithms, benchmark these systems
- Investigate score-level and/or decision-level fusion to improve the detection accuracy compared to the baseline systems

4.2.3 Expected Outcome

- Overview on approaches for score or decision-level fusion
- Benchmark of selected fusion methods
- Comprehensive report including a comparison of the fused score performance against the original algorithms

4.2.4 Reading and other Material

- Priesnitz, et al.: COLFIPAD: A Presentation Attack Detection Benchmark for Contactless Fingerprint Recognition (under review), 2023.
- Kolberg, et al.: COLFISPOOF: A New Database for Contactless Fingerprint Presentation Attack Detection Research, WACV Workshops, 2023.
- PAD scores of various algorithms
- ISO/IEC 30107-1
- DET script

4.3 No-Reference Image Quality Assessment for Contactless Fingerprint Recognition (QFR)(0.7)

Can a no-reference image quality assessment (NR-IQA) precisely assess the quality of contactless fingerprint images?

4.3.1 Background

No-reference image quality assessment refers to algorithms which are able to assess the general quality of arbitrary images. The goal of this project is to test established NR-IQAs on contactless fingerprint samples.

4.3.2 Task

Test different NR-IQAs, e.g. BRISQUE and NIQE, on a contactless fingerprint database.

4.3.3 Expected Outcome

- Research prerequisites for NR-IQA on contactless fingerprints
- Set up and test the chosen NR-IQAs on contactless fingerprints.
- Report sample quality and predictive performance on a given database, e.g. using EDC curves.

4.3.4 Reading and other Material

- D. Varga: No-Reference Image Quality Assessment with Convolutional Neural Networks and Decision Fusion. Applied Sciences 12, 2022
- A. Mittal, et al., No-Reference Image Quality Assessment in the Spatial Domain, in IEEE Transactions on Image Processing, vol. 21, no. 12, pp. 4695-4708, 2012
- A. Mittal, et al., Making a "Completely Blind" Image Quality Analyzer, in IEEE Signal Processing Letters, vol. 20, no. 3, pp. 209-212, March 2013
- Contactless Fingerprint databases
- Fingerprint comparison scores from two systems on the provided contactless fingerprint databases
- Script for computing EDC curves

4.4 Motion Blur Detection (MBD)(0.8)

Create a dataset of images with motion blur effect. Follow the given example. Then, select a motion blur detection algorithm and evaluate its performance on the created dataset.

4.4.1 Background

Motion blur is the blurring of an image due to the movement of the subject or the imaging system. Motion blur is challenging for face recognition systems because it degrades the quality of the captured facial characteristics.

4.4.2 Task

- Analyze the ISO/IEC 29794-1 and ISO/IEC 29794-5 with respect to motion blur
- Use your own camera to create a dataset of real motion blurred face images. Use multiple cameras, if possible. Avoid Smartphone cameras, as they tend to compensate motion![1].
- Use at least one motion blur detection algorithm (or create one yourself) and evaluate its detection performance on the motion blurred images you created. Compare the measures with the high quality reference data set.

4.4.3 Expected Outcome

- The code (open-source frameworks and/or developed code).
- The dataset of blurred images you created with your camera(s).
- A report describing the process, the evaluation results, your observations on the different methods along with your explanation for the results and your thoughts for future work.

4.4.4 Starting Reading and other Material

- Estimation of motion blur parameters using cepstrum analysis: https://ieeexplore.ieee.org/document/5973859
- Review of Motion Blur Estimation Techniques: http://www.joig.org/uploadfile/2014/0414/20140414024045345.pdf
- MotionBlur-detection-by-CNN: https://github.com/Sibozhu/MotionBlur-detection-by-CNN
- High quality reference data set

[1]The data set should contain as many unique subjects (20+) as possible and be captured with consent such that data can be shared for research purposes. A consent form is provided

4.5 Face Occlusion Analysis (FOA)(0.7)

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

4.5.1 Background

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

4.5.2 Task

- Describe state-of-the-art for handling occlusions in the context of face recognition systems
- Create an appropriate database of occluded face images. The database should also contain ground-truth images without occlusions
- Use existing face recognition algorithms and measure the impact of face occlusions, i.e. by comparing the performance of the occluded faces to the performance of the ground-truth images without occlusions.
- Report the results using appropriate ISO/IEC standards

If you have additional time (optional) it could also be interesting to develop an algorithm to detect the occluded face images.

4.5.3 Expected Outcome

- Description of approaches for handling occluded faces in face recognition systems
- A database of face images with and without occlusions
- A performance benchmark investigating the impact of face occlusions on (at least) one open-source face recognition system

4.5.4 Starting, Reading, and other Material

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

4.6 Morphing Attack Potential (MAP)(0.8)

Investigate the threat of morphing attacks on face recognition systems.

4.6.1 Background

A morphed face image is created by combining facial features from at least two distinct subjects. Such morphed face images pose a threat to face recognition systems as potentially all contributing subjects can authenticate against the morphed image. However, not all morphing techniques pose the same threat against face recognition systems. To quantify the threat of morphing techniques, several metrics have been proposed. Recently, in [1], Ferrara et al. proposed a new metric called "Morphing Attack Potential" (MAP), which has the advantage that it is capable of considering multiple face recognition systems and attempts. Your task is to use this metric to evaluate the threat of a provided set of morphed face images against state-of-the-art face recognition systems.

4.6.2 Task

- Select at least two face recognition systems and compute relevant comparison scores [2]
- Use the code in [2] to calculate the MAP metric on a provided set of morphed face images for your selected face recognition systems

If you have additional time it would be interesting to also compare the MAP metric to other morph vulnerability metrics from the literature.

4.6.3 Expected Outcome

- Comprehensive report which, among other things, contains a motivation, description of related work, a morph vulnerability study using MAP, as well as a discussion and conclusion.

4.6.4 Starting, Reading, and other Material

1. M. Ferrara, A. Franco, D. Maltoni, and C. Busch, "Morphing Attack Potential", in IWBF, 2022.
2. https://github.com/matteoferrara/morphing-attack-potential
3. Database of morphed face images
4. U. Scherhag, C. Rathgeb, J. Merkle, R. Breithaupt and C. Busch, "Face Recognition Systems Under Morphing Attacks: A Survey," in IEEE Access
5. ISO/IEC WD 20059

[2] Read the documentation in [2] to figure out what you need to extract for each system

4.7 Face Age Manipulation with Machine Learning (FAM)(0.8)

Select a *personalized text-to-image* model to simulate how facial appearances of subjects change with increasing/decreasing age and evaluate how this affects the face recognition performance.

4.7.1 Background

Recent advancements in deep generative models allow for controlled manipulation of facial attributes, enabling the measurement of the impact of individual factors on recognition system accuracy. This term paper aims to research state-of-the-art text-to-image models and use them to evaluate how face aging affects facial appearances and its impact on the mated comparison scores of a face recognition system.

4.7.2 Task

- Research personalized text-to-image model applicable to face age simulation (e.g., *Dreambooth*).
- Use the best-suited method to simulate the facial appearance under different target ages on a given dataset.
- Evaluate the impact of age on the mated comparison scores of an open source face recognition system.

4.7.3 Expected Outcome

- The code (open-source frameworks and/or developed code) - a link to a git repo with the specific submission commit is even better.
- The dataset with age-simulated face images from the starting database.
- A visual representation of the impact of age on the biometric performance (e.g., score distribution plots)
- A report describing the process, evaluations, and observations on the method along with your explanation for the results and your thoughts for future work.

4.7.4 Starting Reading and other Material

- Dreambooth: N. Ruiz et al. “Dreambooth: Fine tuning text-to-image diffusion models for subject-driven generation”, 2022.
- MagFace (https://github.com/IrvingMeng/MagFace)
- Face images from the FRGCv2 dataset
- ISO/IEC-19795-1 standard
- DET script

4.8 Face Weight Manipulation with Machine Learning (FWM)(0.8)

Select a *personalized text-to-image* model to simulate how facial appearances change when subjects gain/lose weight and evaluate how this affects the face recognition performance.

4.8.1 Background

Recent advancements in deep generative models allow for controlled manipulation of facial attributes, enabling the measurement of the impact of individual factors on recognition system accuracy. This term paper aims to research state-of-the-art text-to-image models and use them to evaluate how the change of body weight affects facial appearances and its impact on the mated comparison scores of a face recognition system.

4.8.2 Task

- Research personalized text-to-image model applicable to weight gain/loss simulation (e.g., *Dreambooth*).
- Use the best-suited method to simulate the facial appearance under weight changes on a given dataset (see starting material).
- Evaluate the impact of weight gain/loss on the mated comparison scores of an open source face recognition system.

4.8.3 Expected Outcome

- The code (open-source frameworks and/or developed code) - a link to a git repo with the specific submission commit is even better.
- The dataset with weight-simulated face images from the starting database.
- A visual representation of the impact of weight on the biometric performance (e.g., score distribution plots)
- A report describing the process, evaluations, and observations on the method along with your explanation for the results and your thoughts for future work.

4.8.4 Starting Reading and other Material

- Dreambooth: N. Ruiz et al. “Dreambooth: Fine tuning text-to-image diffusion models for subject-driven generation”, 2022.
- MagFace (https://github.com/IrvingMeng/MagFace)
- Face images from the FRGC-v2 dataset
- ISO/IEC-19795-1 standard
- DET script

4.9 Develop a New Beauty Photo-filter Database (BPD)(0.7)

Today, many people use smartphone apps or dedicated websites to apply filters to selfie images. This topic will identify popular filters to beautify facial images, apply them to a dataset of facial images and investigate the impact on face recognition systems.

4.9.1 Background

Facial retouching algorithms have become common tools which are frequently applied to improve ones facial appearance, e.g. before sharing face images via social media. Beautification induced by retouching has the ability to substantially alter the appearance of face images and hence might represent a challenge for face recognition and morphing attack detection.

4.9.2 Task

- List and summarize popular recent photo-filters applied to faces (e.g., TikTok filters).
- Select some filters and apply it on a database of facial images
- Investigate the impact of these selfie filters on face recognition systems
- Report the results using appropriate ISO/IEC standards

If you have additional time (optional) it could also be interesting to develop an algorithm to detect the different beautified images.

4.9.3 Expected Outcome

A report which, among other, include the following:

- A detailed summary covering the recent photo-filters
- Creation of a new database using selected photo-filters
- An evaluation report

4.9.4 Starting, Reading, and other Material

- Subset of FERET or FRGCv2 face database
- C. Rathgeb, et al., "Differential Detection of Facial Retouching: A Multi-Biometric Approach," in IEEE Access, vol. 8, pp. 106373-106385, 2020
- ISO/IEC-19795-1 standard
- DET script

4.10 Face Morphing Attack Detection (MAD)(0.8)

Implement a differential morphing attack detection (D-MAD) algorithm.

4.10.1 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. D-MAD algorithms, i.e. algorithms which take as input both a trusted (live capture) and a suspected image, has shown to work well in some cases for detecting morphed images. Your task is to implement or find an existing D-MAD algorithm and evaluate the performance on a given dataset of bona fide and morphed images.

4.10.2 Task

- Implement a method for 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

If you have time it would also be interesting to repeat the evaluation of the trained model where you degrade the quality (e.g., compression, illumination changes, etc.) of the bona fide and morphed images to see how it affects the performance of your system.

4.10.3 Expected Outcome

- An evaluation according to ISO/IEC 30107-3 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

4.10.4 Starting, Reading, and other Material

- Bona fide and morphed images from the FERET and FRGCv2 datasets
- M. Ferrara, et al.: The magic passport. in IEEE International Joint Conference on Biometrics (IJCB), 2014.
- R Raghavendra, et al.: Detecting Morphed Face Images. In 8th IEEE International Conference on Biometrics: Theory, Applications, and Systems, 2016.
- ISO/IEC 30107-3 & DET script

4.11 Face Morphing Capacity (FMC)(0.8)

Explore the capacity of morphed face images.

4.11.1 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.

4.11.2 Task

- Investigate the capacity of realistic morphed face images: How many data subjects could use one single passport?
- Select one or more realistic morphing tools (e.g. NTNUmorpher, UTW, UBO)
- Generate morphed facial images[3] from 2 subjects and check if both subjects can be validated with their probe image.
- Generate morphed facial images from 3,4,5,...,n subject and repeat in each step the recognition validation
- Report the attack potential of the different morphing techniques that you use

4.11.3 Expected Outcome

- Generated data and a comprehensive report including, but not limited to, related work, experimental-setup, results and conclusion

4.11.4 Starting, Reading, and other Material

- subset of FERET, FRGCv2 and FRLL databases
- MagFace (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 30107-1 and ISO/IEC 30107-3

[3] Ideally you should try to create morphs that has good visual quaility, i.e. few artefacts

4.12 Face Beauty Score Implementation (FBI)(0.8)

Implement a hand-crafted method to assess the beauty of a facial image.

4.12.1 Background

Some psychologists claim that the averaging of two faces lead to a more beautiful face. Thus if one would have a robust measure for beauty / attractiveness of a face, one could potentially derive a method for detecting morphed face images.

4.12.2 Task

Implement a hand-crafted method for measuring the attractiveness of facial images. Exploit as described in the literature the geometric proportions of faces. Provide an overview of the literature (for hand-crafted approaches) and augment. Describe your implementation and share it as open-source software. Evaluate the usefulness of such implementations with a plausibility test

- Investigate the literature from psychology, medicine and pattern recognition for face beauty scoring methods
- Seek hand-crafted approaches and implement at least one of these approaches
- Use a robust landmark detector (i.e. ADNet)
- Summarize and compare the approaches found.
- Illustrate the measures for a small set of images (4 subjects, 2 male - 2 female, 2 attractive (i.e Brad Pit) 2 less attractive (i.e. Gérard Depardieu) with 10 images for each subject

4.12.3 Expected Outcome

- A comprehensive implementation and evaluation of an open-source software for measuring the beauty of facial images
- Discuss capabilities, strengths and weaknesses of the surveyed approaches

4.12.4 Starting Reading and other Material

- L. Liang et al.: SCUT-FBP5500: A Diverse Benchmark Dataset for Multi-Paradigm Facial Beauty Prediction
- L. Xu et al.: Hierarchical multi-task network for race, gender and facial attractiveness recognition
- T. Valentine et al.: Why are average faces attractive? The effect of view and averageness on the attractiveness of female faces
- ADNet-landmarks: https://github.com/huangyangyu/ADNet

4.13 Face Beauty Score Benchmark (FBB)(0.6)

Investigate methods to assess the beauty of a facial image.

4.13.1 Background

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 robust measure for beauty / attractiveness of a face, one could potentially derive a method for detecting morphed face images. But how good are those methods?

4.13.2 Task

Benchmark at least two methods for measuring the attractiveness of facial images. Generate a brief overview of the literature. Collect an extensive set of high quality face images for a benchmark of scoring methods. Extensively evaluate the usefulness of such implementations.

- Investigate the literature from psychology, medicine and pattern recognition for face beauty scoring methods
- Seek and apply at least 2 hand-crafted and CNN-based approaches.
- Collect a set of 40 subjects, 20 male - 20 female, 20 attractive (i.e Brad Pit) 20 less attractive (i.e. Gérard Depardieu) with 10 images for each subject
- Ensure that all face images have sufficient good quality (e.g., MagFace quality score)
- Summarize your findings

4.13.3 Expected Outcome

- A comprehensive benchmark of open-source software for measuring the beauty of facial images
- Discuss capabilities, strengths, and weaknesses of the benchmarked approaches

4.13.4 Starting Reading and other Material

- L. Liang et al.: SCUT-FBP5500: A Diverse Benchmark Dataset for Multi-Paradigm Facial Beauty Prediction
- L. Xu et al.: Hierarchical multi-task network for race, gender and facial attractiveness recognition
- L.Xu et al.: Combo Loss for facial attractiveness analysis with squeeze-and-excitation networks.
- T. Valentine et al.: Why are average faces attractive? The effect of view and averageness on the attractiveness of female faces

4.14 Face Image Quality Assessment (FQA)(0.7)

Implement and evaluate one or more face image quality assessment methods to detect the presence of head coverings.

4.14.1 Background

The performance of 2D-image-based face recognition systems depends on the quality of the face images. Being able to assess the quality of single images can consequently be useful in various scenarios, for example when face images are captured for use in travel documents.

This topic is about the implementation and evaluation of methods for the "No head covering" quality element that is included in the current draft of the ISO/IEC 29794-5:202x standard.

4.14.2 Task

- Select suitable face images with and without head coverings from existing databases for tests, or create them yourself.
- Implement one or more methods to detect head coverings.
- Evaluate how well head coverings are detected.
- Optionally evaluate the computational performance.
- Optionally evaluate the impact of head coverings on face recognition performance.

4.14.3 Expected Outcome

- Selected or created test face images.
- One or more "No head covering" quality element implementations.
- Report that describes the method(s) and the evaluation results.
- A Python interface for the method(s).

4.14.4 Starting, Reading, and other Material

- Current draft of ISO/IEC 29794-5:202x.
- ISO/IEC 39794-5:2019, which describes requirements.
- Face image databases.
- "Face Image Quality Assessment: A Literature Survey" for general face image quality assessment information (https://arxiv.org/pdf/2009.01103.pdf).

4.15 Adversarial Attacks on Face Presentation Attack Detection (AAF) (0.8)

Evaluate the impact of several adversarial attack techniques on facial presentation attack detection (PAD) algorithms.

4.15.1 Background

Adversarial attacks are malicious attacks on data that may appear correct at first glance, but cause misclassification in a machine learning process. Face PAD techniques aim on the other hand at determining whether an input sample stems from a live subject or from an artificial copy. Recently PAD methods perform well when the same set of materials or presentation attack instrument (PAI) species are used both to generate the training and testing samples. So far, the impact of applying adversarial attacks on facial PAD algorithms has not been evaluated extensively.

4.15.2 Task

- Investigate adversarial attacks methods. Select and implement some of them. You can start simple by, e.g. adding random noise to the test images
- Evaluate the impact of applying selected adversarial attacks on the performance of facial PAD algorithms.

4.15.3 Expected Outcome

- Implementation of Adversarial Attacks.
- Evaluation of the impact of the above adversarial attacks on facial PAD algorithms.
- Analysis and discussion of results reached.

4.15.4 Starting, Reading, and other Material

- (REPLAY-MOBILE) A. Costa-Pazo et al., The replay-mobile face presentation-attack database. Proc. BIOSIG (pp. 1-7). IEEE, 2016.
- George and Marcel: Deep pixel-wise binary supervision for face presentation attack detection. Proc. ICB, 2019.
- L. J. Gonzalez-Soler et al., On the generalisation capabilities of Fisher vector-based face presentation attack detection, 2021
- Vakhshiteh et al.: Adversarial attacks against face recognition: A comprehensive study. IEEE Access, 9, 2021.
- ISO/IEC 30107-3 & DET script

4.16 Face Anonymisation Experiments (FAE)(0.7)

Conduct experiments with existing methods for anonymisation of facial images.

4.16.1 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.

4.16.2 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.

4.16.3 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. Align your evaluation with appropriate standards. You should, for instance, report DET curves
- Comprehensive report including, but not limited to, experimental setup, the created database, and the results, along with a discussion thereof

4.16.4 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"
- MagFace (https://github.com/IrvingMeng/MagFace) or other state-of-the-art face recognition system
- Subset of the FERET and FRGCv2 facial image database
- DET curve software
- ISO/IEC-19795-1 standard

4.17 Face Stretching Analysis (FSA)(0.7)

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

4.17.1 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.

4.17.2 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.

4.17.3 Expected Outcome

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

4.17.4 Starting, Reading, and other Material

- Subset of face images from the FERET and FRGCv2 database
- MagFace (https://github.com/IrvingMeng/MagFace) or other state-of-the-art face recognition system
- ISO/IEC-19795-1
- DET curve software

4.18 Survey on Adversarial Attacks on Face Recognition Systems (SAF)(0.4)

Conduct a survey of relevant topics on adversarial attacks on face recognition systems.

4.18.1 Background

Face recognition systems based on neural networks and deep learning techniques have achieved great success in recent years. However, some researchers have shown that the outputs and performances of the models can be easily influenced by intentionally adding some noises or perturbations.

4.18.2 Task

Conduct a survey on adversarial attacks on face recognition systems. Motivate your work by introducing what is adversarial attack and pointing out its impact on face recognition systems. Your survey could, e.g. investigate the following questions:

- Which methods exists for generating adversarial attacks against face recognition systems?
- What knowledge of the attacking face recognition system is required by the different attacks (black-box/white-box)?
- What is the result of the attacks on face recognition systems?
- How efficient is the approach (how much time is needed to generate an attack)?
- Which attack is most effective, e.g. how do the attacks compare against each other?

It could also be interesting to apply some of the adversarial attacks on open-source face recognition systems and report the results.

4.18.3 Expected Outcome

- A comprehensive survey of the reviewed approaches.

4.18.4 Starting, Reading, and other Material

- Y. Zhou et al. The Adversarial Attacks Threats on Computer Vision: A Survey
- F. Vakhshiteh et al.: Threat of Adversarial Attacks on Face Recognition: A Comprehensive Survey

4.19 Survey on Detection of Synthetic Face Images (DSF)(0.4)

A comprehensive survey of approaches for detecting synthetic face images

4.19.1 Background

Synthetic face images are images which have been generated, e.g. by using artificial intelligence. It has been shown that such synthetic images are indistinguishable from real images by the human eye. Take a look yourself at this link: https://this-person-does-not-exist.com[4]. As you see it is quite realistic.
As a result, some researchers have proposed methods for detecting such generated synthetic images.

4.19.2 Task

Conduct a survey on existing methods for detecting synthetic face images. Motivate the work by describing how synthetic images can lead to loss of trust in digital content. Your survey can for instance investigate the following:

- Which detection algorithms exists and how do they work?
- How is the algorithms trained and how well do they perform for detecting synthetic face images?
- Are there any limitation of the current algorithms and open problems which needs to be solved?
- Could other approaches be used to prevent the spread of synthetic images, e.g. watermarking?

4.19.3 Expected Outcome

- Comprehensive survey on detection of synthetic face images

4.19.4 Starting, Reading, and other Material

- S.-Y. Wang, et al., CNN-Generated Images Are Surprisingly Easy to Spot... for Now, 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2020
- C. Rathgeb, et al., Handbook of Digital Face Manipulation and Detection: From DeepFakes to Morphing Attacks, Springer, 2022

[4] Refresh the page to see a new synthetic image

4.20 Vulnerability Analysis of Bloom Filters (VAB)(0.4)

Research on biometric template protection schemes based on bloom filters to identify their vulnerabilities and known attacks.

4.20.1 Background

Biometric data are sensitive personal data that require effective protection. Therefore, the ISO/IEC 24745 standard on biometric information protection defines three requirements for secure biometric systems: unlinkability, renewability, and irreversibility. Different approaches have been proposed in the past to design biometric template protection (BTP) systems that meet these requirements. One category of such approaches are bloom filters. The task of this project is to perform a two-step literature review: First, identify recent biometric template approaches using bloom filters. Second, find literature on vulnerabilities and known attacks of the chosen approaches and discuss these with respect to the ISO/IEC 24745 requirements.

4.20.2 Task

- Review literature to find recent BTP schemes using bloom filters.
- For these approaches, review literature that presents attacks or security concerns in the sense of ISO/IEC 24745.
- Discuss vulnerabilities of the reviewed approaches with respect to ISO/IEC 24745.

4.20.3 Expected Outcome

- A taxonomy of vulnerabilities of bloom filter-based BTP in the style of Fig. 2 in: Drozdowski et al., "Computational workload in biometric identification systems: An overview", IET Biometrics, 2019.
- A comprehensive literature review, including in-depth discussion and bibliography.

4.20.4 Starting, Reading, and other Material

- Introduction of: Yasuda et al., "Packed Homomorphic Encryption Based on Ideal Lattices and Its Application to Biometrics", ARES 2013.
- Rathgeb and Uhl: "A survey on biometric cryptosystems and cancelable biometrics", EURASIP 2011.
- Bassit et al.: "Bloom Filter vs Homomorphic Encryption: Which approach protects the biometric data and satisfies ISO/IEC 24745?", BIOSIG 2021.
- ISO/IEC 24745

4.21 Vulnerability Analysis of Cancelable Biometrics (VCB)(0.4)

Research on cancelable biometric template protection schemes to identify their vulnerabilities and known attacks.

4.21.1 Background

Biometric data are sensitive personal data that require effective protection. Therefore, the ISO/IEC 24745 standard on biometric information protection defines three requirements for secure biometric systems: unlinkability, renewability, and irreversibility. Different approaches have been proposed in the past to design systems that meet these requirements. One category of such approaches are cancelable biometrics, referring to irreversible transformations on biometric templates that still allow for an effective computation of the comparison scores. The task of this project is to perform a two-step literature review: First, identify recent BTP approaches within the category of cancelable biometrics (excluding bloom filters, which are covered in topic 4.20). Second, find literature on vulnerabilities and known attacks of the chosen approaches and discuss these with respect to the ISO/IEC 24745 requirements.

4.21.2 Task

- Review literature to find recent approaches to cancelable biometrics.
- For these approaches, review literature that presents attacks or security concerns in the sense of ISO/IEC 24745.
- Discuss vulnerabilities of the reviewed approaches with respect to ISO/IEC 24745.

4.21.3 Expected Outcome

- A taxonomy of vulnerabilities of bloom filter-based BTP in the style of Fig. 2 in: Drozdowski et al., "Computational workload in biometric identification systems: An overview", IET Biometrics, 2019.
- A comprehensive literature review, including in-depth discussion and bibliography.

4.21.4 Starting, Reading, and other Material

- Introduction of: Yasuda et al., "Packed Homomorphic Encryption Based on Ideal Lattices and Its Application to Biometrics", ARES 2013.
- Rathgeb and Uhl: "A survey on biometric cryptosystems and cancelable biometrics", EURASIP 2011.
- ISO/IEC 24745

4.22 Post-Quantum Secure Iris Template Protection (PQI)(0.9)

Implement a previously proposed post-quantum secure iris template protection scheme using a state-of-the art cryptography library.

4.22.1 Background

Biometric data are sensitive personal data that require effective protection over several decades. Therefore, post-quantum cryptography has become popular for biometric template protection (BTP). One of the first post-quantum BTP schemes was proposed for iris verification and identification by Kolberg et al. in 2019. However, their implementation does not apply state-of-the-art cryptographic implementation, which is indicated in their repository as well. The task of this project is therefore to update the implementation made available by Kolberg et al. using a state-of-the art cryptography library that implements the NTRU scheme used in the original work. The preferred language for this topic is C++, not Python.

4.22.2 Task

- Research different cryptographic libraries or **official** reference implementations that implement the NTRU (sometimes called Stehle-Steinfeld) scheme
- Consult with the supervisor of this topic on which library or reference implementation you are planning to use (pia.bauspiess (at) ntnu.no)
- Implement the verification transaction of the original scheme
- For additional contribution: implement identification transaction

4.22.3 Expected Outcome

- Implementation of the scheme by Kolberg et al. using a state-of-the art cryptography library
- Comprehensive report including a comparison of the computational efficiency compared to the original implementation

4.22.4 Starting, Reading, and other Material

- IITD iris database
- Kolberg et al.: Template protection based on homomorphic encryption: Computationally efficient application to iris-biometric verification and identification, IEEE WIFS, 2019. (link to corresponding Github repository in paper)
- ISO/IEC 24745

4.23 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**.

5 Topic assignments

Once you have carefully considered and chosen your research topic you can register your topic on the following website:
https://cloud.h-da.de/apps/polls/s/e1qebD00
Please write your full name in the name field when registering. You can only select a single topic. 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: _____

City, 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?
- The download links for my starting material seem to have expired. How can I fix this?
- 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 would like to cite a statement from the lecture slides in my report. How can I do that correctly?
- 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://cloud.h-da.de/apps/polls/s/e1qebD00`
Please write your full name in the name field when registering. You can only select a single topic. 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. Note that the references are included in the final length of the 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.

The download links for my starting material seem to have expired. How can I fix this?

This is a known cookie issue. Please clear your cache and try again. All download links are valid until the end of the course.

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 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. More recently, AI tools such as Connected Papers or Research Rabbit have been designed to help researchers find related works on a specific topic. Please do not trust these tools blindly, but apply common sense to their results. Note that this list of search engines 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. Generally speaking, a good starting point to a survey topic can be to construct a taxonomy (which will be part of your research contribution) of reviewed approaches in the style of Fig. 2 in: Drozdowski et al., "Computational workload in biometric identification systems: An overview", IET Biometrics, 2019, and to analyze and compare the reviewed works accordingly.

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 08.06.2023 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. Please sign the NDA by hand, either with a digital pen, your mouse, or by printing it out and scanning it again. 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.

I would like to cite a statement from the lecture slides in my report. How can I do that correctly?

The lecture is not a peer-reviewed academic article, and can therefore not be used as a reference. If you wish to cite statements that have been discussed in the lectures, please find a corresponding peer-reviewed publication that supports the statement you wish to make. Please mind that the term paper shall not repeat lecture content, but build on top of the lecture content and highlight your own research contribution. If you however do find yourself in a situation where you require a reference for a statement made in the lecture, you must include a peer-reviewed reference for it

(leaving the statement without a reference is not acceptable and will be considered as plagiarism). A good option is to look in the references to the lectures on the last slide of each session, and to see if the statement is supported by a published work there. The second option is to look for a peer-reviewed reference yourself online. If you are unsure about a concrete reference, you may send an email to the teaching assistants with the statement you are looking to support, the reference with clear indication of the page and paragraph where you would say the reference supports that statement, and we will give you feedback. Please mind that we can only offer this for a limited number of references for each student as we wish to provide the same depth of supervision to all students, the number of which in this course is high.

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**.

9 A Practical Guideline to Academic Writing

As a student in the biometrics course or a thesis student, you are required to deliver a longer piece of academic writing. This Section gives short and simple guidelines for basic principles to mitigate common mistakes. Following the suggestions below will help to increase the quality of your academic writing and thereby your grade, but also to lighten the review workload on your supervisors. Please note that this document is not intended to be a comprehensive guide on academic writing, but a summary of helpful recommendations and formal requirements.

9.1 Structure of an Academic Paper

Your paper or thesis should adhere to the following high-level structure:

- Abstract
- Introduction
- Related work (can be included in the introduction)
- Main body of the paper: this will look different depending on your topic, but usually includes a subset of the following sections:
  - Background
  - Methodology
  - Literature survey (in case of survey topics)
  - Experimental evaluation (including results and discussion)
- Conclusion

Please reach out to your supervisor or the teaching assistants if you have questions on how to adapt this structure to your research topic.

9.2 References

- It is important that you include references for all statements in your paper which are not directly derived from your contribution or the experiments you conducted. These references should be peer-reviewed academic articles.
- Make sure that it is clear which statements are your own and which are founded in previously published work. A clear distinction between your own contribution and established research determines whether a paper is viewed as a plagiarism attempt.
- Please note that the lecture is not a peer-reviewed academic article, and can therefore not be used as a reference. If you wish to cite statements that have been discussed in the lectures, please find a corresponding peer-reviewed publication that supports the statement you wish to make.

- Use peer-reviewed papers as references as much as possible. News articles can be used for simple statistics or as motivation, but not further than that. Instead, please find the official sources.
- If possible, do not use preprints (e.g., from arXiv or eprint) as references, as they are not peer-reviewed. If the paper is also published, then use that publication source.
- For citing with author names, only use last names. For papers with one author, use "Lastname [Ref] describes ...". For papers with two authors, use "Lastname1 and Lastname2 [Ref] describe ...". For papers with more than two authors, use "Lastname1 et al. [Ref] describe ...". Please mind where the dot in "et al." is placed.
- In your bibliography, please make sure that all author names are included and keep the order of the authors as on the original paper.
- Use the citation in the text as you would any other word or symbol, so add spaces before or after if you would do so for a word.
- The citation is part of the sentence and should appear before the period at the end of the sentence.
- References should be cited in text. In other words, if you do not cite it, you do not reference it.
- Please note that the abstract and conclusion should not introduce or contain citations or acronyms.

9.3 Style of Writing

- Write in the passive voice: instead of "I found that", write "it has been found that", where this statement needs to be founded either in your own experiments or in a peer-reviewed reference.
- In some cases, it can be fitting to refer to yourself in the third person as "the author". Please mind to distinguish clearly between "the author of [Ref] describes ..." and yourself as "the author".
- For technical or mathematical phrasing, you can use "we" as in "we define a lattice $\mathcal{L}$ as ..." or "we evaluated the given protocol on the database ...". However, please try to use the passive voice where you can.
- Please maintain a neutral, objective, and respectful tone of voice. Try to avoid the use of the words "very", "extremely", and alike. Often, a well-structured argument gives more meaning to your statement than exaggerated phrasing.
- Please formulate short and concise sentences that are connected with meaningful conjunction words. One sentence should contain one single message to the reader. If a sentence can be divided into two, please do so.

9.4 Figures and Tables

- Each figure or table must have a descriptive caption. Where possible, please keep the caption to one line.
- A figure or table must be referenced in the text. The minimum requirement is a sentence such as "Figure 1 gives an overview of the proposed protocol." following or preceding a description or discussion in the text.
- Figures or tables should be placed at the top or bottom of a page, and should appear on the page they are referenced on, or the next page.
- Please create your own figures and tables, and do not include screenshots from published works. If you recreate or adapt a figure or table from a published work, you must add "(based on [Ref])" or "(adapted from [Ref])" to the caption. Otherwise, this figure will be viewed as plagiarism.
- If you do want to use a figure from a published paper, you must add "(taken from [Ref])" to the caption. Otherwise, this figure will be viewed as plagiarism. Please note that including screenshots of figures and tables is not the preferred approach.

9.5 Formatting

- Please capitalize all major words in any chapter or section headings, following the APA style. You can use the tool Capitalize My Title if you are unsure which words to capitalize.
- If you wish to introduce an abbreviation for a long term, present the term in the style of "Fully Homomorphic Encryption (FHE)" the first time you use it. Thereafter, you can use "FHE".
- The words Figure, Table, Section, and Chapter are capitalized. Please use the `label` and `ref` environments, e.g., cite Figure 1 as `Figure~\ref{fig1}`.
- Please make sure that citations or numbers of figures or tables do not overflow into a new line. You can ensure this by using the "~" symbol in your LaTeX code instead of a white space, for example: `Figure~\ref{fig1}` or `Lastname1 and Lastname2~\cite{lastname1papertitle}`.
- A subsection heading cannot follow immediately after a section heading. Please add a short introductory paragraph beneath the section heading before you introduce the subsection. If you cannot find a fitting description, consider merging the subsection into the section.
- The abbreviations "i.e." and "e.g." are placed between commas, e.g., like this. Alternatively, they can also be used in brackets (i.e., like this). Please use them according to their respective meaning.
- Please spell out abbreviations such as "don't" and write "do not" instead. This also holds for "cannot", "they are", "it is", and alike.
- Please do not use "let's" or "let us".
- Please mind the correct use of quotation marks in LaTeX, which are "these", not "these".

- The word data is plural, not singular.
- Please number all equations.
- Please end all enumerations, bulleted lists and equations with a full stop, unless the sentence continues in the next line.
- Please use the provided Bibtex environment given in the template for your bibliography and make sure that your references are correctly formatted.
- Please use automatic spell-checking tools before you submit.