Biometric Systems - Research Projects

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

Copenhagen, June 6, 2019

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. compare to existing methods

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

Pawel Drozdowski
Email: pawel.drozdowski (at) h-da.de

2 Schedule for Research Assignments

Schedule

Date	Event
June 06, 2019	Research topics for term papers provided
June 11-18, 2019	Lectures
June 17, 2019	Final registration for research topic
June 19-28, 2019	Completion of individual work on research topic
June 28, 2019	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 preferably using the LaTeX typesetting system either in the format used for the Lecture Notes on Informatics (LNI) Word-template:
`http://biosig.org/fileadmin/Files/BIOSIG2019/LNI-Word-Template_en_final.doc`
LaTeX-template:
`http://biosig.org/fileadmin/Files/BIOSIG2019/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 19795-1:2006 Biometric performance testing and reporting. A script for producing DET-curves will be provided in Campusnet.

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 campusnet (`https://www.campusnet.dtu.dk`) on June 28, 2019 (no later then 23.59h). Note that we can not negotiate extensions to this deadline.

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-campusnet:
  `https://www.campusnet.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 three 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 to one individual or one group.

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 assistant 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. Detailed discussions 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 assistant via email. 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.

4.1 Free Fingerprint Recognition Software (FPR)(0.4)

Analysis of free fingerprint recognition software.

4.1.1 Background

Fingerprint recognition software is the basis for numerous access control systems. Today there are not only commercial solutions available. Some free software solutions are available.

4.1.2 Task

- Perform an investigation on open source fingerprint recognition software libraries and software development kits. Briefly describe at least three SDKs and explain your decisions for or against a specific SDK. You can also consider trial versions of commercial SDK that you can find.
- 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 your fingerprint 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.

4.1.3 Expected Outcome

- Report on open source fingerprint recognition software libraries / SDKs and the algorithm used
- Report on biometric performance benchmark

4.1.4 Starting Reading and other Material

- Fingerprint image data FVC2002 database
- ISO/IEC-19795-1
- Code to generate DET curves

4.2 Benchmark Fingerprint Classification Algorithms (FPC)(0.4)

Benchmark fingerprint classification algorithms by performing classification of fingerprint databases and analyze statistical class distributions with respect to existing statistics.

4.2.1 Background

Fingerprint identification systems are used in a wide area of applications in civilian as well as law enforcement contexts. During the identification of subjects within the databases of those systems, pre-selection algorithms can be used to reduce the number of references, to which a given probe has to be compared. One approach for pre-selection is to classify the fingerprint patterns into predefined classes and focus on references that share the same class with the probe during identification. The goal of this paper is to apply selected classification approaches to publicly available fingerprint databases like CASIA or MCYT and create statistics on the class distributions based on the classifier outputs.

4.2.2 Task

- Apply existing classification algorithms to different fingerprint databases
- Create statistics of fingerprint class distributions
- Compare results to given statistics and discuss findings

4.2.3 Expected Outcome

A report containing (but not necessarily limited to):

- Description of the used classification algorithms
- Outline of the databases and their characteristics
- Summary and discussion of the created statistics

4.2.4 Starting Reading and other Material

- Handbook of Biometrics, Handbook of Fingerprint Recognition
- Galar: A survey of fingerprint classification part I: Taxonomies on feature extraction methods and learning models, 2015
- Galar: A survey of fingerprint classification part II: Experimental analysis and ensemble proposal, 2015
- Statistics for comparison will be provided

4.3 Fingerphoto Presentation Attack Detection (FPD)(0.5)

Investigate smartphone based fingerphoto recognition system components that can detect presentation attacks.

4.3.1 Background

Specifically in unsupervised scenarios it is essential that fingerprint sensors can not be spoofed. Examples for such scenarios are mobile payment protocols. Thus an important aspect for the security of a biometric systems is its robustness to artefacts (e.g. fake fingerprints)

4.3.2 Task

Conduct a survey and implement two selected methods for presentation attacks in smartphone fingerphoto based biometrics and how to prevent them.

- Describe different approaches of how a biometric characteristic can be spoofed. Describe briefly presentation attacks for fingerprint recognition.
- Analyse the attack scenarios and try to suggest countermeasures against these attacks.
- Check the literature for published countermeasures.
- Implement and test two methods.
- Collect pros and cons for each of your attack scenarios. Try to weigh the actual risk of such an attack by looking at the estimated time and success probability of creating an artefact. Also include considerations about the number of vulnerable sensors available

4.3.3 Expected Outcome

Report including:

- Survey (with Bibliography), which is aligned to ISO/IEC IS 30107-1
- Describe pro/Cons of the methods for attacks
- Describe and implement countermeasures

4.3.4 Starting Reading and other Material

- BEAT project `https://www.beat-eu.org`
- ISO/IEC IS 30107-1
- ISO/IEC IS 30107-3

4.4 Fingerphoto Comparison Evaluation (FPE)(0.8)

Preprocess at least two finger photo data sets based on a given basedline implementation and compute comparison scores with an off-the-shelve algorithm.

4.4.1 Background

In a touchless-to-touchbased interoperability scenario fingerprints of both domains have to be comparable. In a first stage the biometric performance of touchless fingerprints should be evaluated using a touch based feature extraction and comparision. Due to the heterogeneity data sets the preliminary processing has to be applied to them.

4.4.2 Task

Adapt a given preprocessing pipeline for each data set in order to homogenize it. Apply a given feature extractor to them and compute comparison scores. Evaluate the process and possibly improve it over a few iterations.

4.4.3 Expected Outcome

- Adapted processing pipelines for each data set
- Report of achieved comparison scores
- General performance estimation for touch based comparison of touchless fingerprints

4.4.4 Reading and other Material

- V. Kanhangad, A. Kumar, and D. Zhang, A unified framework for contactless hand verification," IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 1014-1027, 2011.
- Wang, Kejun, et al. "A Preprocessing Algorithm for Touchless Fingerprint Images." 2016.
- Data sets, reference implementations for processing, feature extraction and comparison

4.5 Survey on Machine Learning for Fingerprint Presentation Attack Detection (MLP)(0.5)

Review existing approaches utilising machine learning for fingerprint presentation attack detection (PAD).

4.5.1 Background

Biometric systems are often used for unsupervised authentication in order to accelerate the processing and save personnel expenses. While software attacks require some knowledge of the system and access to inner modules, attacks directed to the sensor can be carried out by eventually any person, without having any knowledge about how the system works. Hence, the most exposed element of the biometric system in terms of security is the sensor. This can be exploited by presenting synthetic artefacts (e.g. gummy fingers, photographs, etc.) to the capture device in order to alter its normal functioning, in the so-called Presentation Attacks (PA). Therefore, secure systems require a Presentation Attack Detection module to judge whether the presented characteristic stems from a living person or not.

4.5.2 Task

Conduct a survey on machine learning for fingerprint PAD and describe the results of your findings. Motivate your work by pointing out the risks of biometric recognition without PAD. Describe different approaches by answering the following questions:

- What machine learning algorithm is used? (SVM, DNN etc.)
- Which capturing method is used?
- What type of features are extracted?
  What type of features serve as input to the machine learning?

4.5.3 Expected Outcome

- Survey (with Bibliography) of the reviewed approaches.

4.5.4 Starting Reading and other Material

- E. Marasco and A. Ross. A Survey on Antispoofing Schemes for Fingerprint Recognition Systems. ACM Computing Surveys (CSUR), 47(2):28, 2015.
- C. Sousedik and C. Busch. Presentation Attack Detection Methods for Fingerprint Recognition Systems: A Survey. Biometrics, IET, January 2014.

4.6 Pore Based Fingerprint Presentation Attack Detection (PPD)(0.8)

Investigate fingerprint presentation attack detection methods based on high quality images and pore extraction.

4.6.1 Background

It is essential that fingerprint sensors can not be spoofed, and this is specially relevant for unsupervised scenarios (e.g., access control, or verification using your smartphone). Therefore, we need to develop methods to detect artefacts. When creating a fingerprint fake overlay with someone else's fingerprint, it is very challenging to recreate the sweat pores – these features can be thus used to detect the attacks.

4.6.2 Task

Conduct a survey and describe the results of methods for presentation attacks detection based on sweat pore extraction and implement one of the best performing methods, preferable based on deep learning.

- Describe different approaches of how a biometric characteristic can be spoofed. Describe briefly presentation attacks for fingerprint recognition.
- Check the literature for published countermeasures, with special focus on pore extraction methods.
- Implement (preferably Python + Keras) and evaluate one of the deep learning based pore extraction methods on a provided database

4.6.3 Expected Outcome

Report including:

- Short survey (with Bibliography) on pore extraction and its relationship with fingerprint Presentation Attack Detection, which is aligned to ISO/IEC IS 30107-1
- Describe pro/cons of the methods
- Implementation (preferably Python + Keras) and evaluation of one of the pore extraction methods on a provided database

4.6.4 Starting Reading and other Material

- R. Labati, A. Genovese, et al. A novel pore extraction method for heterogeneous fingerprint images using convolutional neural networks. Pattern Recognition Letters, vol. 113, pp. 58-66, 2018
- H.U. Jang, D. Kim, et al. DeepPore: fingerprint pore extraction using deep convolutional neural networks. IEEE Signal Processing Letters, 24(12), pp. 1808-1812, 2017
- ISO/IEC IS 30107-1
- ISO/IEC IS 30107-3

4.7 Fingerprint Image Enhancement (FIE)(0.6)

Perform image enhancements to fingerprint images to determine the influence on recognition accuracy.

4.7.1 Background

A crucial step in fingerprint recognition is that of correct minutia extraction. This requires the fingerprint image to be of sufficient quality. Enhancing a fingerprint image prior to feature extraction may recover regions where minutia could not otherwise be extracted, thus leading to a potential increase in recognition performance.

4.7.2 Task

Given a fingerprint feature extractor and comparator determine the impact of the application of fingerprint enhancement methods to the comparison score. The enhancement techniques may come from literature as well as your own ideas. To use multiple methods is strongly encouraged. Suggested methodology: 1) compute comparison scores on provided fingerprint images to find a baseline performance. 2) apply at least three enhancement methods to the images and recompute the comparison scores and subsequently performance metrics. Determine the influence of the enhancement techniques and discuss the result.

4.7.3 Expected outcome

- DET curves of the comparison scores from images which were not enhanced and of images which were enhanced.
- Report on result and implementation of the applied fingerprint enhancement methods.

4.7.4 Starting Reading and other Material

- Fingerprint images from the FVC2002 database
- Code to generate DET curves
- Fingerprint feature extraction and comparison pipeline (provided as virtual machine)

4.8 Selection of Touchless Fingerprint Images in a Mobile Setup (FTI)(0.4)

Develop a collection of algorithms which is able to select high quality finger images from a finger photo.

4.8.1 Background

Touchless fingerprint recognition is a fast-growing research topic and achieves a high user acceptance and usability. A flexible and user-friendly capturing process is achieved by an autonomous process which is able to select the presented finger and estimate the images quality e.g. regarding sharpness. Other aspects like the amount of presented fingers, distance between the camera and the hand should be taken into account, too.

4.8.2 Task

- Evaluate different approaches for image quality estimation and their applicability on touchless fingerprints.
- Integrate the most suitable algorithms in a given smartphone app using Android and OpenCV.
- Test your proposed processing workflow.

4.8.3 Expected Outcome

- A collection of images quality estimation algorithms suitable for touchless fingerprint images.
- A report on the improvements achieved by the proposed algorithms.

4.8.4 Starting Reading and other Material

- Yang, Bian, Guoqiang Li, and Christoph Busch. "Qualifying fingerprint samples captured by smartphone cameras." 2013
- Wang, Kejun, et al. "A Preprocessing Algorithm for Touchless Fingerprint Images." 2016.
- Vincent Muehler: Simple Hand Gesture Recognition using OpenCV and JavaScript, 2017 (OpenCV Node.js Tutorial Series on www.medium.com)

4.9 Fingerphoto Sample Quality (FPQ)(0.8)

Analyze fingerprint images from Smartphones and evaluate fingerprint image sample quality and compare with existing approaches.

4.9.1 Background

In April 2016 NIST published a second generation of measures of fingerprint image quality, which is designed to predict the biometric performance of minutia-based fingerprint recognition systems. The definition and methodology of NIST Fingerprint Image Quality (NFIQ 2.0) is documented its implementation is publicly available.

4.9.2 Task

Setup an operational version of NFIQ2.0 on your system. Analyze how the quality values are correlated with recognition performance across a dataset of fingerprint photos collected from a current Smartphone. The dataset should contain 10 fingers from at least 10 subjects captured in 2 sessions.

4.9.3 Expected Outcome

- Collection of at least 2x100 fingerprint images
- Report with evaluation of NFIQ2.0 values and correlation with recognition accuracy

4.9.4 Starting Reading and other Material

- NISTIR 7151: Fingerprint Image Quality
- P. Grother and E. Tabassi: Performance of Biometric Quality Measures
- M. Olsen et al: Finger image quality assessment features? definitions and evaluation.available online: `http://digital-library.theiet.org/content/journals/10.1049/iet-bmt.2014.0055s`
- `http://www.nist.gov/itl/iad/ig/development_nfiq_2.cfm`

4.10 Multi-Sample Fusion for Contact-less Finger Photos (MSF)(0.8)

Contact-less hand-based recognition systems can capture multiple finger photos at the time of biometric enrolment or authentication using a mobile phone. In such case multiple biometric samples can be fused in order to improve the recognition accuracy of the biometric system.

4.10.1 Background

A super-template implies a superior feature set which is generated from multiple fingerprint images by combining information from different inputs. In recent years, there have been several efforts to develop robust approaches for contact-less hand-based biometrics. The main difference between contact-based and contact-less systems lies in the significant intraclass variations resulting from the absence of any contact or guiding surface to restrict such variations. Such variation might be suppressed using multi-biometric fusion techniques.

4.10.2 Task

- Investigate options to fuse multiple templates of finger photos from a data subject
- Collect a small test database of at least 10 different subject to test your method

4.10.3 Expected Outcome

- Report the implemented system and results of tests.

4.10.4 Starting Reading and other Material

- V. Kanhangad, A. Kumar, and D. Zhang, A unified framework for contact-less hand verification," IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 1014-1027, 2011.
- A. Kumar and Y. Zhou, Contactless Fingerprint identification using level zero features," in CVPR 2011 WORKSHOPS, pp. 114-119, 2011.
- Ryu C., Han Y., Kim H. (2005) Super-template Generation Using Successive Bayesian Estimation for Fingerprint Enrollment. Audio- and Video-Based Biometric Person Authentication. AVBPA 2005. Lecture Notes in Computer Science, vol 3546.

4.11 Fingerprint Image Validation (FIV)(0.7)

Investigate and evaluate methods on detecting the presence of a fingerprint in an image and apply the methods on the FVC2002 dataset and non-fingerprint images.

4.11.1 Background

On fingerprint acquisition devices it is not always evident how exactly to place the finger, e.g. some subjects will place only the tip of a finger on the sensor plate. By determining the degree that the captured image resembles a fingerprint it is possible to reject or accept a biometric sample for further processing at an early stage.

4.11.2 Task

Analyze the SIVV method described in NISTIR 7599. Compose a dataset using FVC2002 and various non-fingerprint images which are selected from other sources. Apply the SIVV method on the composed dataset and develop or evaluate other methods for fingerprint image validation and compare the performance.

4.11.3 Expected Outcome

- Survey report
- Dataset
- Prototype software implemented in programming language of choice

4.11.4 Starting Reading and other Material

- NISTIR 7599: A 1D Spectral Image Validation/Verification Metric for Fingerprints
- Fingerprint image data FVC2002 database

4.12 Finger Knuckle Recognition (FKR)(0.8)

Investigate the processing steps from finger image showing the knuckles to templates that can be compared with biometric references.

4.12.1 Background

Finger knuckle surface measurements have been suggested recently as biometric method. However there is only little experience with that biometric method to be applied on images taken with a Smartphone.

4.12.2 Task

Investigate and optionally implement the processing pipeline that is necessary to build up a finger knuckle recognition system. Specifically investigate feature extraction based on the BSIF method. The prototype should be evaluated with finger knuckle images from at least 100 fingers (10 subjects).

4.12.3 Expected Outcome

- Prototype software implemented in programming language of choice

4.12.4 Starting Reading and other Material

- IITD-Knuckle
- Code to generate DET curves
- L. Zhang et. al: Finger-Knuckle-Print: A new biometric identifier
- A. Kumar: Personal identification using finger knuckles
- J. Kannala and E. Rahtu: BSIF: Binarized statistical image features, ICPR 2012

4.13 Finger Presentation Attack Detection Based on Knuckle Photos (FKP)(0.8)

It has been shown that finger knuckle based person recognition is possible, for instance using BSIF features. However, as any other biometric characteristics, presentation attacks (PAs) can be launched on the sensor, which decreases the security provided by biometric systems.

4.13.1 Background

Investigate and implement the processing pipeline from finger knuckles for presentation attack detection (PAD) purposes. The prototype should be evaluated with finger knuckle images from at least 100 fingers (10 subjects).

4.13.2 Task

- Investigate the feasibility of using BSIF or alternative features as well for PAD purposes
- Collect a small test database of at least 10 different subject to test your method: it should comprise the bona fides and the corresponding PAs with: an overlay, a printed image and a replay on a smartphone or tablet.

4.13.3 Expected Outcome

- Prototype software implemented preferably in Python, alternatively in Matlab or C.
- Report the implemented system and results of tests.

4.13.4 Starting Reading and other Material

- L. Zhang et. al: Finger-Knuckle-Print: A new biometric identifier
- A. Kumar: Personal identification using finger knuckles
- J. Kannala and E. Rahtu: BSIF: Binarized statistical image features, ICPR 2012
- Code to generate DET curves and to extract BSIF features from the finger knuckles.

4.14 Survey on Neural Networks for Presentation Attack Detection (NNP)(0.5)

Review existing approaches utilising (deep) neural networks (DNN) for presentation attack detection (PAD) for different biometric characteristics.

4.14.1 Background

Given that in many applications, biometric systems are used for unsupervised authentication, an eventual attacker may try to manipulate the sensor in order to gain unauthorised access. These attacks, known in the literature as presentation attacks (PAs) or spoofing, can be carried out by presenting synthetic artefacts (e.g. gummy fingers, photographs, etc.) to the capture device in order to alter its normal functioning. To prevent such scenarios and increase the security of the system, a Presentation Attack Detection (PAD) module is required to judge whether the presented characteristic stems from a living person (bona fide presentation) or not (PA).

4.14.2 Task

Conduct a survey on PAD techniques based on (deep) neural networks and describe the results of your findings. Motivate your work by pointing out the risks of biometric recognition without PAD. Describe different approaches by answering the following questions:

- Which DNN is used?
- What kind of samples are used? (e.g., visible or NIR images, video sequence)
- Is there any pre- or post-processing of the samples or features?
- Is there any freely available implementation of the method?

4.14.3 Expected Outcome

- Survey (with Bibliography) of the reviewed approaches.

4.14.4 Starting Reading and other Material

- D. Menotti, G. Chiachia, A. Pinto, W. R. Schwartz, H. Pedrini, A. X. Falcao, A. Rocha. Deep representations for iris, face, and fingerprint spoofing detection. IEEE Transactions on Information Forensics and Security, 10(4), 864-879, 2015.
- R. F. Nogueira, R. de Alencar Lotufo, R. C. Machado. Fingerprint liveness detection using convolutional neural networks. IEEE Transactions on Information Forensics and Security, 11(6), 1206-1213, 2016.

4.15 Survey on Anomaly Detection for Unknown Presentation Attack Detection (ADP)(0.5)

Review existing approaches utilising anomaly detection techniques for the detection of unknown presentation attacks for different biometric characteristics.

4.15.1 Background

Given that in many applications, biometric systems are used for unsupervised authentication, an eventual attacker may try to manipulate the sensor in order to gain unauthorised access. These attacks, known in the literature as presentation attacks (PAs) or spoofing, can be carried out by presenting synthetic artefacts (e.g. gummy fingers, photographs, etc.) to the capture device in order to alter its normal functioning. Different approaches to prevent such attacks (known as PAD) have been presented in the literature. In spite of their effectiveness in detecting a particular kind of PA (e.g., gummy finger fabricated with silicone), their vulnerability to previously unseen (e.g., gummy finger fabricated with play-doh) has been shown. Since anomaly detection techniques focus on modelling a particular class (in our case bona fide or live presentations), and detecting any deviations from it in other samples (i.e., PAs), it is foreseen as an effective method to detect unknown PAs.

4.15.2 Task

Conduct a survey on anomaly detection techniques in general, and on their application to biometrics or PAD in particular. Motivate your work by pointing out the risks of biometric recognition without PAD and the more complex challenge of detecting unknown PAs. Describe different approaches by answering the questions:

- Which anomaly detection algorithm is used?
- What kind of samples are used? (e.g., visible or NIR images, video)
- Is there any pre- or post-processing of the samples or features?
- Is there any freely available implementation of the method?

4.15.3 Expected Outcome

- Survey (with Bibliography) of the reviewed approaches.

4.15.4 Starting Reading and other Material

- V. Chandola et al. Anomaly detection: A survey, 2009
- O. Nikisins et al. On Effectiveness of Anomaly Detection Approaches against Unseen Presentation Attacks in Face Anti-Spoofing, 2018

4.16 SMR reversibility attack with Neural-Networks (SNN)(0.8)

Train an open-source deep neural network (DNN) to reverse SMRs to its minutiae-vector.

4.16.1 Background

The ISO 24745:2011 requires biometric reference probes to be stored in irreversible templates. One way to obtain irreversible template of fingerprint or vein minutiae is to use Spectral Minutiae Representation (SMR) as stated by the Authors, since it relies on multiple irreversible mathematical operations. In the last couple of years, the ongoing research in neural networks yielded powerful and efficient new algorithms and patterns. Those powerful neural networks could be used to attack biometric templates ans systems which, amongst others, applies to the SMR, too.

4.16.2 Task

The task is to chose one or multiple DNN and to train it with (synthetic or extracted) minutiae and their corresponding SMR. Then it should be analysed if the DNN is able to reproduce an approximation of the original minutiae vector when given an SMR.

4.16.3 Expected Outcome

- Proof-of-concept of the reversibility attack.
- Evaluation of reversibility attack vector on SMR potential (with e.g. comparison score-distributions of reversed minutiae vectors and original minutiae vectors).

4.16.4 Starting Reading and other Material

- Haiyun Xu; Raymond N.J. Veldhuis; Spectral Minutiae Representations for Fingerprint Recognition
- A dataset of 39.600 fingerprint minutiae (and other meta-data) with their corresponding SMR (SML and SMC) is provided.
- A SMR comparator written in python is provided.

4.17 Vein Liveness Detection (VLD)(0.5)

Vein recognition systems gain popularity in real life applications, for example many Japanese banks use this biometric modality to secure the ATM access. Besides the popularity of vein recognition, research in this topic is often restricted by financial interests - products on the market are usually black boxes, existing algorithms and techniques not revealed by vendors.

4.17.1 Background

Biometrics is commonly considered as a promising alternative to token-based or knowledge-based authentication schemes as a biometric characteristic can neither been lost nor forgotten by the individual. However a large number of nowadays biometric sensors is not resistant against presentation attacks with replicates from a biometric characteristic.

4.17.2 Task

Conduct a survey on how to generate artefacts vein patterns and describe how to design possible countermeasures.

4.17.3 Expected Outcome

- Report on presentation attacks on vein recognition systems
- Report on presentation attack detection on vein recognition systems

4.17.4 Starting Reading and other Material

- ISO/IEC IS 30107-1
- ISO/IEC IS 30107-3
- Junichi Hashimoto: Finger Vein Authentication Technology and its Future
- L. Wang et al: Infrared imaging of hand vein patterns for biometric purposes

4.18 Vein Image Quality (VIQ)(0.5)

Vein recognition systems gain popularity in real life applications, for example many Japanese banks use this biometric modality to secure the ATM access. The quality of captured samples is a critical aspect in biometric systems.

4.18.1 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 vascular images, before they are stored in a reference database.

4.18.2 Task

Conduct a survey on currently available methods for quality estimation for vascular data (i.e. fingervein and handvein images). Try to develop own approaches and test how well they perform on publicly available vascular data sets.

4.18.3 Expected Outcome

- A comprehensive state-of-the-art survey (with bibliography) of vascular image quality estimation and the effects of vascular image quality on the biometric performance
- A comparative assessment of the surveyed approaches
- Discuss open problems and future research perspectives in the area

4.18.4 Starting Reading and other Material

- D. Hartung: Quality Estimation for Vascular Pattern Recognition
- Junichi Hashimoto: Finger Vein Authentication Technology and its Future
- L. Wang et al: Infrared imaging of hand vein patterns for biometric purposes

4.19 Vein Skeleton Extraction Methods (VSE)(0.4)

Vein recognition is popular in research and is already present in real life application as Japanese ATMs. After capturing vein images, the most common way is to extract the vein skeleton from these. Devices that perform many recognitions should be able to do so in real-time such that subjects do not need to wait unnecessarily.

4.19.1 Background

Several methods are able to obtain the vein skeleton from NIR vein images. How do those techniques differ in quality and execution time?

4.19.2 Task

Implement different methods to extract the vein skeleton from NIR images. Test your implementations on identical datasets to benchmark the execution time and report visible quality differences. Examples of extraction methods are: Repeated Line Tracking, Maximum Curvature, Principle Curvature, Mean Curvature, and Wide Line Detection.

4.19.3 Expected Outcome

- Implementations of several vein skeleton extraction methods
- Report including description of the methods and a comparison between those methods

4.19.4 Starting Reading and other Material

- Example of Maximum Curvature implementation
- Vein SDK `http://www.wavelab.at/sources/OpenVein-SDK/`
- Bob Signal Processing Toolkit `https://www.idiap.ch/software/bob/`
- C. Kauba, B. Prommegger, A. Uhl. The Two Sides of the Finger-An Evaluation on the Recognition Performance of Dorsal vs. Palmar Finger-Veins. In International Conference of the Biometrics Special Interest Group (BIOSIG) 2018.

4.20 Hand-based Biometric Recognition (HBR)(0.5)

Touch-less hand-based biometric recognition is more likely to be accepted as it is more hygienic and comfortable to the user. What is the current state-of-the-art in contact-less hand-based biometric recognition?

4.20.1 Background

Hand-based biometric characteristics (fingerprints, palm prints, finger knuckles, etc.) represent well-known physiological biometric characteristics, which have been used for automated recognition of individuals for several decades. In recent years, there have been several efforts to develop robust approaches for contact-less hand-based biometrics. The main difference between contact-based and contact-less systems lies in the significant intraclass variations resulting from the absence of any contact or guiding surface to restrict such variations. Such variations can result from the rotational and translation variations, projective distortion, scale variations or blurring due to the hand movement during the image acquisition.

4.20.2 Task

- Starting from a literature research an overview should be conducted

4.20.3 Expected Outcome

- Comprehensive survey (with bibliography) on the state-of-the-art of contact-less hand-based biometric recognition technologies

4.20.4 Starting Reading and other Material

- V. Kanhangad, A. Kumar, and D. Zhang, A unified framework for contact-less hand verification," IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 1014-1027, 2011.
- A. Kumar and Y. Zhou, Contactless Fingerprint identification using level zero features," in CVPR 2011 WORKSHOPS, pp. 114-119, 2011.
- A. Morales, M. A. Ferrer, and A. Kumar, Towards contactless palmprint authentication," IET Computer Vision, vol. 5, no. 6, pp. 407-416, 2011

4.21 Face Presentation Attack Detection (APD)(0.5)

Investigate face recognition system components that can detect presentation attacks.

4.21.1 Background

Specifically in unsupervised scenarios it is essential that face sensors can not be spoofed. Examples for such scenarios are un-attended border crossing or mobile payment. Thus an important aspect for the security of a biometric systems is its robustness to artefacts (e.g. face masks)

4.21.2 Task

Conduct a survey and describe the results of methods for presentation attacks in biometrics and how to prevent them.

- Describe presentation attacks for face recognition.
- Analyse the attack scenarios and try to suggest countermeasures against these attacks.
- Collect pros and cons for each of your attack scenarios. Try to weigh the actual risk of such an attack by looking at the estimated time and success probability of creating an artefact.

4.21.3 Expected Outcome

Report including:

- Survey (with Bibliography), which is aligned to ISO/IEC IS 30107-1
- Pro/Cons of the methods related to scenarios
- Get hold of a face mask to be used in attacks

4.21.4 Starting Reading and other Material

- TABULA RASA project
  `https://www.tabularasa-euproject.org/`
  spoofing competitions, publications
- BEAT project `https://www.beat-eu.org`
- ISO/IEC IS 30107-1
- ISO/IEC IS 30107-3

4.22 Single Image Super Resolution for Face Recognition (FSR)(0.7)

Investigate and evaluate image super resolution techniques on facial images.

4.22.1 Background

In the recent past different researchers demonstrated the feasibility of creating high quality face images from low quality face images, in particular by using deep learning. It is of interest whether these methods enable the application of face recognition is unconstrained scenarios where only low quality images are available. The goal of this project is to benchmark different face recognition systems on low quality face images before and after the application of different open-source single image super resolution methods.

4.22.2 Task

- Creation of low-quality/low-resolution database by application of various scaling factors
- Application of available super resolution techniques
- Benchmark and evaluation of face recognition systems on the databases, i.e. the original one, low-resolution one(s), and super-resolution one(s)

4.22.3 Expected Outcome

- A report describing the created database, the used super resolution techniques, and the results
- Discussion of the results, as well as open problems/challenges and future perspectives in the area
- All the written and used code/scripts

4.22.4 Starting Reading and other Material

- Glasner et al. Super-resolution from a single image
- Ledig et al. Photo-Realistic Single Image Super-Resolution Using a Generative Adversarial Network
- FaceNet: Face recognition using Tensorflow `https://github.com/davidsandberg/facenet`
- Subset of FERET face database
- DET curve software

4.23 Face Morphing Capacity (FMC)(0.8)

Explore the capacity of morphed face images.

4.23.1 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.

4.23.2 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)

4.23.3 Expected Outcome

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

4.23.4 Starting Reading and other Material

- FEI database
- OpenFace `https://github.com/cmusatyalab/openface`
- 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

4.24 Face Eye Segmentation and Morphing Detection (FHS)(0.7)

Explore the eye region as information to detect morphed face images.

4.24.1 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. In order to detect morphed images, the analysis of the eye area seems promising, as many morphing attacks leave iris shadows.

4.24.2 Task

- Analyze the suitability of the eye region as a characteristic to distinguish morphed images from normal face images (bona fide images)
- 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.
- Develop a robust segmentation method for the eye region.
- Analyze if information from the eye region can help to distinguish morphed images from normal face images.
- Report the capability of the segmentation method.

4.24.3 Expected Outcome

- A comprehensive report on the segmentation method and its benefit for morphing detection.

4.24.4 Starting Reading and other Material

- FEI database
- OpenFace (open source face recognition tool), `https://github.com/cmusatyalab/openface/blob/master/docs/setup.md`
- 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

4.25 Face Image Quality (FIQ)(0.8)

Investigate metrics that measure the quality of facial images.

4.25.1 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 facial images, before they are stored in a reference database.

4.25.2 Task

Analyze the ISO/IEC 29794-1 (framework), ISO/IEC 29794-5 (face) and ISO/IEC 29794-6 (iris) and investigate, which of the suggested metrics are indeed predicting biometrics accuracy. Suggested methodology: 1) compute comparison scores on provided face images to find a baseline of recognition performance. 2) implement a selection of suggested face quality metrics. Specifically include `GREY_SCALE_UTILISATION` and `SHARPNESS` from 29794-6 standard 3.) analyze, if the metrics are predicting recognition accuracy. Also the BRISQUE method shall be investigated.

4.25.3 Expected outcome

- Implementation of selected face quality metrics
- Graphs showing the relation between quality metrics and the biometric performance (e.g. correlation or error-versus-reject-curve)

4.25.4 Starting Reading and other Material

- ISO/IEC 29794-1,5,6
- Face images from CASIA V5
- openCV face recognition (or other open source software)
- P. Grother and E. Tabassi,, Performance of Biometric Quality Measures, IEEE TIFS, 2007
- Script to compute the ERC curve
- A. Mittal, A. K. Moorthy, and A. C. Bovik, Blind/referenceless image spatial quality evaluator, in Proceedings ASILOMAR-2011.

4.26 Face Anonymisation Survey (FAS)(0.5)

Conduct a survey of existing methods for anonymisation of facial images.

4.26.1 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.

4.26.2 Task

Conduct a survey on currently available methods for anonymisation of facial images. Additionally, investigate adversarial methods for reversing the effects of the anonymisation filters. Also include a comprehensive overview of existing open-source software in the area.

4.26.3 Expected Outcome

- A comprehensive state-of-the-art survey (with bibliography) of methods and existing open-source software for anonymisation and de-anonymisation of facial images
- Discussion of capabilities, and strengths and weaknesses of the surveyed approaches
- Discussion of the open problems and future research perspectives in the area

4.26.4 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"

4.27 Face Anonymisation Experiments (FAE)(0.8)

Conduct a experiments with existing methods for anonymisation of facial images.

4.27.1 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.

4.27.2 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.

4.27.3 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

4.27.4 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"
- FaceNet: Face recognition using Tensorflow `https://github.com/davidsandberg/facenet`
- Face Detection: OpenCV, Dlib and Deep Learning `https://www.learnopencv.com/face-detection-opencv-dlib-and-deep-learning-c-python/`

- Subset of the FERET facial image database
- DET curve software

4.28 Face Reenactment using Free Software (FRF)(0.8)

Conduct a survey on and experiments with face reenactment software.

4.28.1 Background

As a result of research interest in increasing video-realism of synthetic humans, many new generation techniques have been developed in recent years. Some of these techniques have caught the public interest and several projects for automating the process are being developed and many tools are being made available on the internet. The process of replacing the facial movements of a person in a video is called reenactment, and combined with fake voice generation techniques such as impersonation can result in convincing fake videos.

4.28.2 Task

Conduct a survey on publicly available tools for manipulation of identity and behaviour of people in a video. Investigate the extent to which it is possible to generate reenactment videos by combining these free software.

4.28.3 Expected Outcome

- A report on the existing publicly available tools.
- Demonstration of reenactment by a combination of existing free software

4.28.4 Starting Reading and other Material

- Dale, Kevin, et al. "Video face replacement." ACM Transactions on Graphics (TOG) 30.6 (2011): 130. (`https://youtu.be/rTvdvNNiCVI`)
- Anonymous, (2019), GitHub repository, `https://github.com/deepfakes/faceswap`
- Marek Kowalski, (2019), GitHub repository, `https://github.com/MarekKowalski/FaceSwap`

4.29 Face Stretching Analysis (FSA)(0.7)

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

4.29.1 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.

4.29.2 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 recognition algorithm and measure the impact of stretching.
- Collect your own data (from public source) and generated a stretched database with controlled stretching parameters (from mild to severe) in both horizontal and vertical direction.
- Report your results using the metrics specified in the ISO/IEC standard and compare your own results with the results form your literature survey.

4.29.3 Expected Outcome

- Report on the current algorithmic approaches to handle stretching in the area of face recognition.

4.29.4 Starting Reading and other Material

- openCV face recognition (or other open source software)
- ISO/IEC-19795-1

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

Analysis of free 2D face recognition software

4.30.1 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.

4.30.2 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
- 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.

4.30.3 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

4.30.4 Starting Reading and other Material

- `http://www.face-rec.org`
- ISO/IEC-19795-1
- Code to generate DET curves
- Face images from CASIA V5

4.31 Benchmarking Facial Soft-Biometric Extractors (BFE)(0.4)

Find and benchmark open-source (must run locally, not in the cloud/online) software for extraction of soft-biometrics from facial images.

4.31.1 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.

4.31.2 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(s))
- 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

4.31.3 Expected Outcome

A report containing (but not necessarily limited to):

- A benchmark and comparative assessment of the tested approaches

The used code:

- The open-source frameworks
- Any additional scripts written for the benchmark

4.31.4 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

4.32 Occlusion Detection in Facial Images (ODF)(0.7)

Find open-source (must run locally, not in the cloud/online) or develop own software for detection of occlusions (e.g. glasses, reflections, shadows, strong make-up, accessories etc.) in facial images.

4.32.1 Background

Occlusions and accessories can deteriorate the biometric performance of a facial recognition system. It is therefore of interest to automatically detect them in order to further process or reject such images.

4.32.2 Task

- Find open-source software or develop own for detection of a set of facial image occlusions.
- Find or create an appropriate database with groundtruth for testing the algorithms
- Perform tests and report/compare the accuracy of the software
- Discuss open problems and future research perspectives in the area

4.32.3 Expected Outcome

A report containing (but not necessarily limited to):

- A benchmark and comparative assessment of the tested approaches

The used code:

- The code (open-source frameworks and/or developed code)
- Any additional scripts written for the benchmark

4.32.4 Starting Reading and other Material

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

- A. Dantcheva *et. al.* What Else Does Your Biometric Data Reveal? A Survey on Soft Biometrics
- Handbook of Face Recognition
- ISO/IEC 19795-1

4.33 Deep Learning in Facial Recognition (DLF)(0.5)

Conduct a state-of-the-art survey on use of deep learning in facial recognition.

4.33.1 Background

Deep learning is a rapidly evolving field of research with many potential applications. In recent years, traditional approaches to facial recognition have largely been superseded by deep learning methods. The goal of this paper is to survey the existing methods and to perform a comparative assessment, e.g. by discussing their recognition rates, computational load, and other properties.

4.33.2 Task

- Conduct comprehensive literature survey (with bibliography) about use of deep learning in facial recognition
- Evaluate and compare the results achieved by the surveyed approaches
- Discuss open problems and future research perspectives in the area

4.33.3 Expected Outcome

A report containing (but not necessarily limited to):

- A comprehensive state-of-the-art survey (with bibliography) on deep learning-based facial recognition
- A comparative assessment of the surveyed approaches
- Where available, links to the repositories of the frameworks/pre-trained models released by the researchers

4.33.4 Starting Reading and other Material

- Handbook of Biometrics, Handbook of face recognition
- "FaceNet: A Unified Embedding for Face Recognition and Clustering"
- ISO/IEC 19795-1

4.34 3D Face from Video (TFV)(0.8)

Face recognition is a very popular biometric approach, which reaches good biometric performance metrics given frontal poses and controlled lighting conditions. The quality of Image material and video material is usually very poor and not suitable for identification purposes.

4.34.1 Background

The analysis of image and video material showing the same face with varying distances and varying head-poses and expressions may be used to parametrize an integrated 3D Model, which then may be used for biometric approaches.

4.34.2 Task

Conduct an extensive literature survey and analyze the current state of the art for approaches to create 3D face models from video.

4.34.3 Expected Outcome

- Report on the current algorithmic approaches to create 3d face models from video sequences and approaches to use these models for face recognition.
- Demonstrate with open source or personal implementation that the approach works

4.34.4 Starting Reading and other Material

- Hanan A. et.al.: A Biometric Database with Rotating Head Videos and Hand-drawn Face Sketches, In Biometrics: Theory, Applications, and Systems (BTAS), 2009.
- Canavan, et.al.: Face Recognition by Multi-Frame Fusion of Rotating Heads in Videos, In Biometrics: Theory, Applications, and Systems (BTAS), 2007., pp.1-6
- Xin, L.et.al.: Automatic 3D Face Modeling from Video. In IEEE International Conference on Computer Vision (ICCV), 2005.
- Blanz, V. and Vetter, T.: Face Recognition Based on Fitting a 3D Morphable Model. IEEE Trans. Pattern Anal. Mach. Intell. (PAMI), 2003, pp. 1063-1074

4.35 Multi/Cross-Spectral Iris Recognition Survey (MIS)(0.5)

Conduct a survey on multi-spectral and cross-spectral iris recognition methods.

4.35.1 Background

Most iris recognition systems rely on images acquired in a relatively narrow range (700-900 nm) of the light spectrum. In recent years, some research has been conducted into utilising wavelengths other than the near-infrared, namely visible and far-infrared. This research investigated the option of using the other wavelengths for recognition and other purposes on their own, or by fusing the information from multiple spectra (multi-spectral) or the feasibility of recognition between the different spectra (cross-spectral).

4.35.2 Task

Conduct a survey on multi-spectral and cross-spectral iris recognition. Among other matters, provide an overview of the existing research datasets, methods for multi and cross spectral recognition, as well as discuss the potential benefits/use cases of utilising multi-spectral information. Discuss the feasibility and efficacy of cross-spectral methods.

4.35.3 Expected Outcome

- A comprehensive state-of-the-art survey (with bibliography) of multi-spectral and cross-spectral iris recognition methods, including an overview of the available research datasets and the biometric performance results
- Discussion of capabilities, and strengths and weaknesses of the surveyed approaches, as well as potential application areas for multi-spectral data
- Discussion of the open problems and future research perspectives in the area

4.35.4 Starting Reading and other Material

- Ross et al. "Exploring multispectral iris recognition beyond 900nm"
- Nalla et al. "Toward More Accurate Iris Recognition Using Cross-Spectral Matching"

4.36 Eye Detection from Images on Smartphones (EDS)(0.4)

Implement eye detection on Android based smartphones.

4.36.1 Background

The challenges of environmental impact on biometrics can be overcome by employing more robust biometric characteristic - iris. In order to obtain the iris information, the first task consists in detecting the eye region from image on smartphone or live camera feed. Possible approaches include using Haar cascade eye detector from OpenCV for Android.

4.36.2 Task

1. Implement sample OpenCV face detector on Android.
2. Detect the eye region for both eyes and save the eye region image in a specified location.
3. Repeat the capture process if not satisfactory.

4.36.3 Expected Outcome

- Given a face image or live camera feed, the Android code should be able to detect the eye region and save it to specified location.

4.36.4 Starting Reading and other Material

- Roman Hosek - Android eye detection updated for OpenCV 2.4.6 :
  `http://romanhosek.cz/android-eye-detection-updated-for-opencv-2-4-6/`
- OpenCV for Android
  `http://opencv.org/platforms/android.html`

4.37 Visible Iris Quality Estimation (VIE)(0.7)

Evaluate the existing iris quality metrics in visible spectrum and benchmark them against the NIR iris quality metrics.

4.37.1 Background

The gaining interest in the visible spectrum iris recognition has lead to large scale iris data collection. In the case of NIR iris, the ISO quality metrics are used to evaluate the quality of iris image acquired. This work will evaluate the suitability of existing visible spectrum iris quality metrics and benchmark it against the NIR quality metrics.

4.37.2 Task

- Evaluate the visible spectrum iris metrics.
- Evaluate the NIR spectrum iris metrics.
- Report the suitability of NIR metrics for visible spectrum iris.

4.37.3 Expected Outcome

- Evaluation of visible spectrum and NIR iris quality metrics

4.37.4 Starting Reading and other Material

- ISO/IEC 29794-1, -6
- P. Grother and E. Tabassi, Performance of Biometric Quality Measures, IEEE TIFS, 2007
- Script to compute the ERC curve
- Proenca, H. (2011). Quality assessment of degraded iris images acquired in the visible wavelength. Information Forensics and Security, IEEE Transactions on, 6(1), 82-95.
- PolyU Cross Spectral Iris dataset

4.38 Iris Presentation Attack Detection (IPD)(0.5)

Investigate iris recognition system components that can detect presentation attacks.

4.38.1 Background

Specifically in unsupervised scenarios it is essential that iris sensors can not be spoofed. Examples for such scenarios are un-attended border crossing or mobile payment. Thus an important aspect for the security of a biometric systems is its robustness to artefacts (e.g. printed contact lenses)

4.38.2 Task

Conduct a survey and describe the results of methods for presentation attacks on iris recognition systems and how to prevent them.

- Describe different approaches of how a biometric characteristic can be spoofed. Describe briefly spoofing attacks for iris recognition.
- Analyse the attack scenarios and try to suggest countermeasures against these attacks.
- Collect pros and cons for each of your attack scenarios. Try to weigh the actual risk of such an attack by looking at the estimated time and success probability of creating an artefact. Also include considerations about the number of vulnerable sensors available

4.38.3 Expected Outcome

Report including:

- Survey (with Bibliography), which is aligned to ISO/IEC IS 30107-1
- Describe Pro/Cons of the methods scenarios for attacks

4.38.4 Starting Reading and other Material

- TABULA RASA project `https://www.tabularasa-euproject.org/` spoofing competitions, publications
- BEAT project `https://www.beat-eu.org`
- ISO/IEC IS 30107-1
- ISO/IEC IS 30107-3

4.39 Evaluate Generative Adversarial Networks for Iris Sample Reconstruction (GNI)(0.9)

Review existing approaches generative adversarial networks (GAN) for iris sample reconstruction.

4.39.1 Background

Given the progress of deep learning, it has been shown that realistic face images can be generated. Investigate and evaluate, if you can use generative adversarial networks to reconstruct realistic iris images from a given iris codes, that can be used for successful recognition.

4.39.2 Task

Conduct a survey on generative adversarial networks techniques and find a suitable open source implementation. Analyse existing use cases for GAN. Apply a GAN to reconstruct iris samples. Describe the results of your findings. Describe different approaches by answering the following questions:

- Which GAN is used?
- What kind of reconstruction methods are used?

4.39.3 Expected Outcome

- Survey (with Bibliography)
- Evaluation report of the reviewed approaches

4.39.4 Starting Reading and other Material

- T. Karras, S. Laine, T. Aila: A Style-Based Generator Architecture for Generative Adversarial Networks, arxiv.org, 2019.

4.40 Eye Liveness Indicator (ELI)(1.0)

Analyse the state of the art in the area of eye gaze / eye movement detection methods as an application for liveness detection in biometric systems. Moreover evaluate the pupil dilation in a challenge response scenario (ie. illumination with LED)

4.40.1 Background

Liveness detection should be a component of a sophisticated biometric system. It is the process to detect whether a biometric sample was taken from a human being living at the time of capture. Such methods could also be used to detect whether the biometric sample was taken from an artificially generated biometric characteristic. An eye gaze, eye movement detection or pupil dilation could be added as additional interactive liveness detection method to cope with such attacks.

4.40.2 Task

Conduct a survey and describe the detection methods. Distinguish between methods which need additional hardware to detect the movement and such methods which are based on video streams. Apply the EVM magnification method to enhance movements and try to detect them. Use a smartphone as capture device.

4.40.3 Expected Outcome

- Survey on detection methods
- Implementation of the EVM method
- Report on the evaluation and comparison results

4.40.4 Starting Reading and other Material

- A. Bulling, J. Ward, H. Gellersen and G. Troester: "Eye movement analysis for activity recognition", in Proceedings of the 11th international conference on Ubiquitous computing, (2010)
- K. Raja, R. Raghavendra, C. Busch: "Video Presentation Attack Detection in Visible Spectrum Iris Recognition Using Magnified Phase Information", in IEEE Transactions on Information Forensics and Security (TIFS), June, (2015)

4.41 Ear Recognition using Deep-Learning (EDL)(0.8)

Implement a simple ear recognition system, that uses a dep learning for verification or identification of people.

4.41.1 Background

In forensics, the outer ear is one of the most important traits, the forensic experts concentrate on, when searching for proves of identity. However, there are currently no methods for automatically retrieving identities from ear images. Your task will be to investigate the suitability of deep learning for automatic ear recognition. You will be provided with a small dataset for testing and evaluating your system.

4.41.2 Task

- Conduct literature and public software survey
- Write a program that uses a deep learning to recognize people by their ears.

4.41.3 Expected Outcome

- Brief explanation of the core ideas behind deep learning
- A program that decides whether to samples belong to the same person or not. A database will be provided
- Report about the results.

4.41.4 Starting Reading and other Material

- Y. LeCun: Deep Learning - Review, Nature, 2015
- A Pflug, C Busch: Ear biometrics: a survey of detection, feature extraction and recognition methods, IET Biometrics, 2012
- IITD-Ear dataset

4.42 Cross-modal Synchrony for Audiovisual Person Authentication (CMS)(0.5)

Conduct a literature survey on uses of cross-modal (audiovisual) synchrony for presentation attack detection.

4.42.1 Background

Audiovisual person authentication systems increase the recognition performance by processing the information on both the face and voice modalities. In an attack to such systems, the attacker may attempt to generate the face and voice presentations independently. As a result, the synchrony between modalities may be absent and can provide further clues for presentation attack detection (PAD).

4.42.2 Task

Conduct a survey on the existing PAD methods incorporating face-voice synchrony. Categorize, describe, and analyze feature extraction and synchrony detection methods.

4.42.3 Expected Outcome

- A survey on PAD methods utilizing cross-modality synchrony including details about the methods used for feature extraction and synchrony detection

4.42.4 Starting Reading and other Material

- Bredin, Herve, and Gerard Chollet. "Audio-visual speech synchrony measure for talking-face identity verification." 2007 IEEE International Conference on Acoustics, Speech and Signal Processing-ICASSP'07. Vol. 2. IEEE, 2007.
- Boutellaa, Elhocine, et al. "Audiovisual synchrony assessment for replay attack detection in talking face biometrics." Multimedia Tools and Applications 75.9 (2016): 5329-5343.

4.43 Keystroke Dynamics Database Quality (KDQ)(0.5)

4.43.1 Background

Results in papers on biometrics are often hard to compare because researchers use their own database. In KD some standard databases are made available, but there is a large diversity in characteristics of these databases, some with lower and some with higher quality

4.43.2 Task

- Make an overview of available KD databases
- Apply a number of known analysis techniques to each of the databases to determine the quality of them

4.43.3 Expected Outcome

- List and description of available databases
- Report on quality of the available databases

4.43.4 Starting Reading and other Material

- Killhoury and Maxion: Comparing Anomaly-Detection Algorithms for Keystroke Dynamics
- ISO/IEC 29794-1

4.44 Copy vs Free Text typing (CPY)(0.8)

4.44.1 Background

In Continuous Authentication one finds various ways to perform experiments. In some cases the user can simply do his/her daily business, while in others there is more control on the activity of a user. Behaviour might however change in a situation where a user is restricted to a specific task. In this case we will investigate how the behaviour of a person changes when he is forced to retype (copy) a given text, versus the behaviour when he/she can freely type.

4.44.2 Task

- Define an experiment to collect data
- Collect experimental data
- Perform analysis on the collected data

4.44.3 Expected Outcome

- Collected dataset
- Report containing analysis of the differences and commonalties of the copy versus free typing style.

4.44.4 Starting Reading and other Material

- Bergadano et al.: User authentication through keystroke dynamics

4.45 Pattern Recognition using Homomorphic Encryption (PRH)(0.5)

For a wide variety of applications, which require manipulation of sensitive or confidential data, privacy preserving algorithms play an important role. Whereas traditional cryptographic techniques (e.g., RSA) allow no operation on the encrypted domain, Homomorphic Encryption algorithms (e.g., Paillier cryptosystem) do provide a framework for carrying out computations in the encrypted domain, requiring no decryption.

4.45.1 Background

Biometric recognition algorithms rely ultimately on machine learning and statistical modelling algorithms (e.g., SVM, GMM). Given the high sensitivity of biometric data, it is of the utmost importance to handle only protected templates, using for example Homomorphic Encryption techniques. This task is about application of the homomorphic encryption to the wider field of pattern recognition, which includes both statistical modelling and machine learning.

4.45.2 Task

Conduct a survey and describe the results of research already done in this area. Point out the advantages and disadvantages of using homomorphic encryption for pattern recognition.

4.45.3 Expected Outcome

Report including:

- Survey (with Bibliography)
- Pro/Cons of use of homomorphic encryption for pattern recognition.

4.45.4 Starting Reading and other Material

- C. Fontaine and F. Galand: A Survey of Homomorphic Encryption for Non-specialists
- P. Failla: Privacy preserving processing of biometric templates by homomorphic encryption
- M. Aliasgari et al.: Secure computation of hidden Markov models and secure floating-point arithmetic in the malicious model
- Other papers can be searched via IEEE paper search

4.46 DNA Analysis - State of the Art Survey (DNA)(0.5)

Forensic techniques has used DNA for quite some time. With the implementation of the Pruem treaty the exchange of DNA data becomes more relevant.

4.46.1 Background

Forensic genetics using deoxyribonucleic acid (DNA) profiling comprise a number of important applications. Examples are the investigation of biological stains to obtain evidence for the presence of an alleged perpetrator at the crime scene by comparing the genetic profiles from crime scene samples of human origin to those of potential stain donors, the identification of unknown corpses in the context both of natural death and of crime or immigration, paternity testing, and mass disaster. In the last 20 years, forensic molecular genetics has evolved from a rapidly developing field with changing technologies into a highly recognized and generally accepted forensic science, leading to the establishment of national DNA databases from individuals such as suspects, convicted offenders and crimes stains, as permitted by national legislation. The methodology has become quite reliable and the analytical equipment has reached a high level of automation.

4.46.2 Task

Conduct an extensive literature survey and analyse the current state of the art. Provide a detailed technology description of the recognition methods, for example based on Short Tandem Repeats (STR) and single nucleotide polymorphisms (SNPs), or others. Survey some of the most recent advancements in the field, such as fast DNA sequencing technologies. Discuss the advantages and disadvantages of DNA as a biometric characteristic. Discuss the potential for (near) real-time usage of DNA for authentication purposes (also outside of the forensics context), as well as other promising avenues of future research in the field.

4.46.3 Expected Outcome

- Detailed descriptions of technologies associated with DNA-based identification of individuals and a discussion of DNA as a biometric characteristic
- A description of the recent advances in the field along with an extensive discussion thereof

4.46.4 Starting Reading and other Material

- Interpol - Handbook on DNA data and practice
- ISO/IEC: DNA data interchange format, 2013

4.47 Electric Activity-based Biometrics Survey (EBS)(0.5)

Conduct a survey on the use of electrocardiography (ECG) and electroencephalography (EEG) or other similar electric activity-based technologies for biometric recognition.

4.47.1 Background

EEG and ECG can be used to record the electrical activity of the heart and brain, respectively. Those signals have been shown to possess enough discriminative power to distinguish between individuals.

4.47.2 Task

Conduct an extensive literature survey and analyse the current state of the art. Provide a detailed technology description of the existing recognition methods, the features they used, along with the achieved biometric performances. Discuss the advantages, disadvantages, and limitations of electric activity-based biometric modalities. Discuss the potential of such technologies for biometric recognition and/or continuous authentication, emphasising the real-world (potential or existing) applications.

4.47.3 Expected Outcome

A report containing (but not necessarily limited to):

- A comprehensive state-of-the-art survey (with bibliography) on electric activity-based biometric technologies
- A description of the most prominent methods and a comparative assessment of the surveyed approaches including the achieved biometric performances
- Discussion of the potential and limitations of electric activity-based technologies for biometric recognition and/or continuous authentication, as well as the open challenges/problems, future research avenues and potential/existing real-world applications in the area

4.47.4 Starting Reading and other Material

- da Silva et al. "ECG Biometrics: Principles and Applications"
- Gui et al. "Exploring EEG-based Biometrics for User Identification and Authentication"

4.48 Retina Recognition Survey (RRS)(0.5)

Conduct a survey on retina-based biometrics.

4.48.1 Background

The retina biometrics capture and analyse the layer of blood vessels located at the back of the eye. Said blood vessels form unique patterns, which can be used to distinguish between individuals.

4.48.2 Task

Conduct an extensive literature survey and analyse the current state of the art. Provide a detailed technology description of the existing recognition methods, the features they used, along with the achieved biometric performances. Discuss the advantages, disadvantages, and limitations of retina as a biometric characteristic, as well as existing and potential real-world applications of this technology.

4.48.3 Expected Outcome

A report containing (but not necessarily limited to):

- A comprehensive state-of-the-art survey (with bibliography) on retina as a biometric characteristic
- A description of the most prominent methods and a comparative assessment of the surveyed approaches including the achieved biometric performances
- Discussion of the potential and limitations of retina recognition, as well as the open challenges/problems, future research avenues and potential/existing real-world applications in the area

4.48.4 Starting Reading and other Material

- Lajevardi et al. "Retina Verification System Based on Biometric Graph Matching"
- Borgen et al. "Visible-Spectrum Biometric Retina Recognition"

4.49 Workload Reduction in Identification Systems (WRI)(0.5)

Conduct a state-of-the-art survey on biometric identification mode workload reduction for a biometric characteristic of choice.

4.49.1 Background

The quickly growing size of biometric deployments (e.g. the Indian Aadhaar project) confers many diverse challenges, one of which is system efficiency in the identification mode. A naïve implementation of a biometric system in identification mode requires 1:N template comparisons for a lookup. As the number of enrolled subjects (N) increases, the computational load and probability of false positive occurrences quickly become unacceptable. Over time, many approaches for reducing the number of necessary template comparisons have been proposed by the research community.

4.49.2 Task

- Choose one biometric characteristic (e.g. fingerprint or face, **not** iris) and conduct an extensive literature survey about workload reduction in the identification scenario
- Evaluate and compare the results achieved by the surveyed approaches

4.49.3 Expected Outcome

A report containing (but not necessarily limited to):

- A comprehensive state-of-the-art survey (with bibliography) on workload reduction in biometric identification for the chosen characteristic
- A comparative assessment of the surveyed approaches
- Discussion of the trade-off between workload reduction and biometric performance

4.49.4 Starting Reading and other Material

- J. Daugman: Biometric decision landscapes
- Handbook of Biometrics; Handbook of fingerprint/face recognition
- ISO/IEC 19795-1

4.50 Simple Biometric Features (SBF)(0.7)

In some home-like applications simple features, such as weight and length, may be sufficient for identifying people or verifying identities from a small user group. In this assignment the performance and usability of these type of features is to be investigated.

4.50.1 Background

Simple features can often be measured unobtrusively and may be good enough for identifying people or verifying identities from a small user group. Examples can be found in Jam Jenkins and Carla Ellis. Using Ground Reaction Forces from Gait Analysis: Body Mass as a Weak Biometric. Fifth International Conference on Pervasive Computing. Toronto, Canada. May 2007.

4.50.2 Task

Define a set (typically about 5) weak biometric features that can be collected easily by simple means such as scales, rulers, etc. Collect a reasonably large set of these features from colleague students and relatives. Make sure to measure enough sample from each individual, say 10 to 20, with some time lapse (about one week) between subsets. Implement one or more recognition systems in programming language of choice. Analyze by means of experiments the usefulness of these features for verification and identification. Include the effect of time lapse between the feature collection in you analysis. Pay attention to recognition performance, user friendliness and other aspects. Analyze the contribution of the features to the recognition performance.

4.50.3 Expected Outcome

- Simple Biometric Features Test Report
- Data set
- Recognition module

4.50.4 Starting Reading and other Material

- J. Jenkins and C. Ellis. Using Ground Reaction Forces from Gait Analysis: Body Mass as a Weak Biometric. Fifth International Conference on Pervasive Computing. Toronto, Canada. May 2007.

4.51 Synthetic Data Generation (SDG)(0.5)

Conduct a survey of available (open-source and commercial) software for generation of synthetic biometric data.

4.51.1 Background

Acquiring sufficiently large datasets of biometric data is costly and time consuming. An often used approach for large-scale testing is to use synthetically generated data. Additionally, synthetic data can be used to conduct presentation attacks on biometric systems.

4.51.2 Task

Conduct a survey on currently available methods for generation of synthetic biometric data (images and/or feature vectors). If necessary, restrict the search by selecting a few biometric characteristics only.

4.51.3 Expected Outcome

- A comprehensive state-of-the-art survey (with bibliography) on synthetic generators of biometric data
- Discussion of capabilities, and strengths and weaknesses of the surveyed approaches
- Discuss open problems and future research perspectives in the area

4.51.4 Starting Reading and other Material

- N. Orlans: "A Survey of Synthetic Biometrics: Capabilities and Benefits"
- SFinGe (Synthetic Fingerprint Generator)

4.52 Information Fusion Survey (IFS)(0.2)

Conduct a survey on methods for information fusion in multi-biometric systems.

4.52.1 Background

By fusing information from multiple sources the discriminative power of a biometric system can be substantially increased. There are opportunities for fusing information at various levels of the biometric processing pipeline (e.g. scores, decisions, features, signal, etc.).

4.52.2 Task

Conduct an extensive literature survey and analyse the current state of the art. Explore the fusion methods at the different levels of the biometric processing pipeline and provide a comparative assessment of their potential advantages and disadvantages, as well as their impact on the biometric performance. Discuss the open challenges and future research avenues in the area. **Focus especially on the more recent publications and methods.**

4.52.3 Expected Outcome

A report containing (but not necessarily limited to):

- A comprehensive state-of-the-art survey (with bibliography) on information fusion in biometrics
- A description of the most prominent methods and a comparative assessment of the surveyed approaches including the achieved biometric performances
- Discussion of the open challenges/problems and future research avenues in the area

4.52.4 Starting Reading and other Material

- Ross and Jain "Information fusion in biometrics"
- Ross "Handbook of Multibiometrics"
- Jøsang "Subjective Logic"
- Jain et al. "Score normalization in multimodal biometric systems"
- ISO/IEC TR 24722:2015(en) Information technology - Biometrics - Multimodal and other multibiometric fusion
- Ross and Jain "Information fusion in biometrics"

4.53 Survey on Biometrics and Blockchain (BBC)(0.5)

Analyze the use of Biometrics and Blockchain.

4.53.1 Background

The Blockchain technology seems to be spreading to various applications. In some cases the replicate functionality that is already well implemented in a centralised architecture. In other cases Blockchain can provide tangible advantages. Biometrics was identified in theses application, the question is, how this information can be used to strengthen blockchain based applications. Further distributed biometric systems could be designed using blockchains. But as the research in biometric science progresses and new modalities are identified, an interesting question is how can this be exploited and how will this shape the future in related fields?

4.53.2 Task

Identify not only state of the art applications of biometrics in blockchain applications and investigate also future trends. Perform a survey on the scientific literature and write a structured report about your findings.

4.53.3 Expected Outcome

- Structured literature and application survey

4.53.4 Starting Reading and other Material

- A. Jain et al.: Handbook of Biometrics

4.54 Automatic Authorship Identification (AAI)(0.8)

Conduct a survey and experiments on automatically identifying authors of textual samples.

4.54.1 Background

Any written text contains information about the writing style and as a result the identity of the author of the text. Authorship identification is the task of extracting identity-related information from a given text. The success of natural language processing (NLP) methods has been demonstrated for authorship identification. Identification of the author of a text has applications ranging from forensics to plagiarism detection. Furthermore, authorship identification can be used in online communication as a continuous authentication mechanism and account compromise detection.

4.54.2 Task

Conduct a survey on the existing literature on authorship identification. Demonstrate the performance of a selection of methods on Twitter data.

4.54.3 Expected Outcome

- A report containing a survey on the literature of authorship identification along with experimental results on short-text Twitter data.

4.54.4 Starting Reading and other Material

- Houvardas, John, and Efstathios Stamatatos. "N-gram feature selection for authorship identification." International conference on artificial intelligence: Methodology, systems, and applications. Springer, Berlin, Heidelberg, 2006.
- Brocardo, Marcelo Luiz, et al. "Authorship verification for short messages using stylometry." 2013 International Conference on Computer, Information and Telecommunication Systems (CITS). IEEE, 2013.
- `https://data.world/bkey/politician-tweets`

4.55 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://doodle.com/poll/5c6cu7fwe7tcxiyr`
Please write your full name in the name field when registering. 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 USB-stick or via download link. Before you can get the data - please print, sign and scan the NDA contained at the end of this document. Once I 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

I am participating in the Course Biometric Systems (02238). I acknowledge that software / sensitive biometric data provided by the instructor Christoph Busch 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: _____