BRNO UNIVERSITY OF TECHNOLOGY
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

FACULTY OF INFORMATION TECHNOLOGY
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

DEPARTMENT OF INTELLIGENT SYSTEMS
ÚSTAV INTELIGENTNÍCH SYSTÉMŮ

DEEPFAKE DETECTION FRAMEWORK

FRAMEWORK PRO DETEKCI DEEPFAKES

MASTER'S THESIS
DIPLOMOVÁ PRÁCE

AUTHOR **Bc. JAN BERNARD**
AUTOR PRÁCE

SUPERVISOR **Mgr. KAMIL MALINKA, Ph.D.**
VEDOUCÍ PRÁCE

BRNO 2022

BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Master's Thesis Assignment

140642

Institut: Department of Intelligent Systems (UITS)
Student: **Bernard Jan, Bc.**
Programme: Information Technology and Artificial Intelligence
Specialization: Cybersecurity
Title: **Deepfake Detection Framework**
Category: Security
Academic year: 2022/23

Assignment:

1. Learn about deepfakes (voice and video). Explore the current state of deepfakes detection methods (voice and video).
2. Learn about the technologies needed to create web extensions and technologies for creating scalable server applications.
3. Learn about existing deepfake detection solutions (e.g. other commercial web browser plug-ins)
4. Design an extensible framework (server-client or client-only) for deepfakes detection (support for at least 3 detection methods (voice and video)). Design a web extension for deepfakes detection that will use this framework. The solution should support multiple browsers and allow the detection of displayed content and uploaded files.
5. Implement the tool according to the design.
6. Test the functionality and reliability of the resulting implementation. Perform testing on at least two independent publicly available deepfakes datasets.
7. Discuss usability, detection efficiency and possible extensions.

Literature:

Puspita Majumdar, Akshay Agarwal, Mayank Vatsa, and Richa
Singh, “Facial retouching and alteration detection,” in Handbook of Digital Face Manipulation and Detection, pp. 367–
387. Springer, 2022
FIRC Anton a MALINKA Kamil. The dawn of a text-dependent society: deepfakes as a threat to speech verification systems. In: Brno: Association for Computing Machinery, 2022

Requirements for the semestral defence:
Items 1 to 4.

Detailed formal requirements can be found at https://www.fit.vut.cz/study/theses/

Supervisor: **Malinka Kamil, Mgr., Ph.D.**
Consultant: Ing. Anton Firc
Head of Department: Hanáček Petr, doc. Dr. Ing.
Beginning of work: 1.11.2022
Submission deadline: 17.5.2023
Approval date: 3.11.2022

Abstract
Do tohoto odstavce bude zapsán výtah (abstrakt) práce v anglickém jazyce.

Abstrakt
Do tohoto odstavce bude zapsán výtah (abstrakt) práce v českém (slovenském) jazyce.

Keywords
deepfake, framework, deepfake detection, containerazation, web plugin

Klíčová slova
deepfake, framework, detekce deepfake, kontejnerizace, webový doplňek

Reference
BERNARD, Jan. *Deepfake Detection Framework*. Brno, 2022. Master's thesis. Brno University of Technology, Faculty of Information Technology. Supervisor Mgr. Kamil Malinka, Ph.D.

Deepfake Detection Framework

Declaration

I hereby declare that this Master's thesis was prepared as an original work by the author under the supervision of Mgr. Kamil Malinka Ph.D. The supplementary information was provided by Ing. Anton Firc. I have listed all the literary sources, publications and other sources, which were used during the preparation of this thesis.

. . . .

Jan Bernard

January 8, 2023

Acknowledgements

Here it is possible to express thanks to the supervisor and to the people which provided professional help (external submitter, consultant, etc.).

Contents

Chapter 1

Introduction

- deepfake is buzzword (no agreed-upon technical definition) - still growing thread for sociaty
- huge research over past years - reason for creating this framework

Chapter 2

Deepfakes

The creation of fake media and their detection have been a problem since photography was invented. Digital photography or video with tools such as GIMP, Adobe Photoshop or Adobe After Effects allows more people to create fakes than before, still some experience in this area is needed. Media that have been modified or otherwise manipulated are called synthetic media, and they do not depend on whether it is an analogue or digital medium. Deepfakes also fall under this category [6]. Tools powered by deep learning allow unexperienced users to easily create trusted fakes.

The quality of deepfakes reached a level when a trained person or even an experienced researcher in this field has a problem of spotting them. This fast development allows creating realistically looking assets to art photography or movie production, unfortunately, it can be used for malicious purposes like creating fake porn videos to blackmail people or manipulate public via fake news. There are many use cases where deepfakes can be applied.

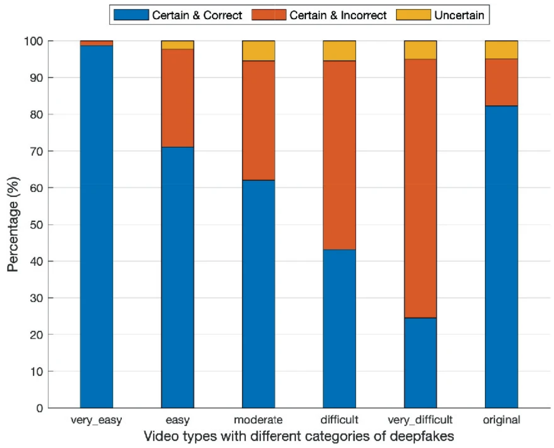
It is putting huge pressure on researchers to develop new forensics tools or any technology which will prevent malicious usage of deepfakes. As mentioned before, creating fakes is not new, and a whole field of study engaged in spotting fakes and developing techniques over 15 years. Despite continuous research efforts in the past, the advent of deep learning changed the rules of the game. [15]

2.1 Human capabilities of deepfake detection

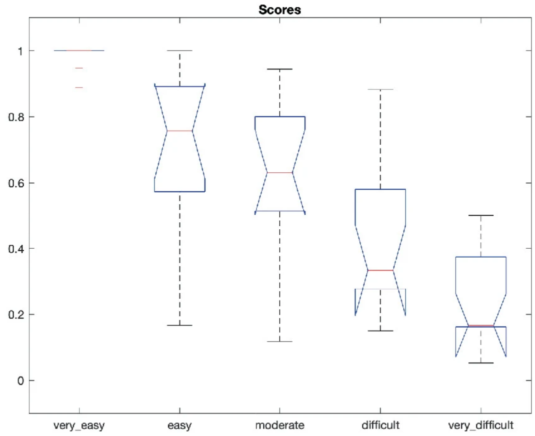
The human ability to recognize fake materials from the originals is in contradiction to their quality. Korshunov and Marcel confirmed this in their research. They created a questionnaire containing several videos, and the subject (interviewee) had to answer after watching the video whether the person in the video was genuine, fake, or they are uncertain. The videos were manually divided into five categories (very easy, easy, moderate, difficult, and very difficult, original).

Videos were split into several categories manually by researchers probably without usage of any metrics but based on their experience and feelings. Afterwards ANOVA test shows there is an overlap in several categories, so several videos could be moved to different category. However, the categories are still significantly different.

The results of test in Fig. 2.1 certainly demonstrate that people's recognition ability decreases significantly as the quality of deepfakes increases. Also, the audience of this test knows they are looking for fakes, otherwise we can expect worse results if there will be unsuspected audience (e.g. deepfakes on social media). It is quite alarming that the correct answers in the category of "very easy" reach only 71,1 %. The quality of deepfake increases over time, thus it can be expected that human recognition ability will continue to decrease. [9]



(a) Subjective answers



(b) ANOVA test

Figure 2.1: Subjective answers and median values with error bars from ANOVA test for different deepfake categories. Retrieved from [9].

Another research tested only recognition of audio tracks and they were comparing humans versus computer programmes. Attendees had a correct classification between fakes and origins 67 % after the first several rounds. Their accuracy increased while listening and answering to more tracks, but the value stabilizes to 80 %. On average, trained AI performs about 10 % better than human, but this result highly depends on difference of learning and test dataset. Still, it shows that the computer can outperform humans in spotting deepfakes. [12]

2.2 Potentional risks

Humans are not good at recognizing deepfakes, but "why should we be worried?". Almost every technology humankind created could be used for good or bad – deepfake is no exception. There are plenty different deepfake categories, and each has its own attack vector or use case. This section is describing potential risks of those categories and their closer description will be covered in next section 2.3.

Deepfakes are about gaining someone's trust or influence him. For the last couple of years there has been an increasing trend of scamming people, mostly via phone or computer [2]. Targeting only one person/victim, for example, to gain their money or information. Those attacks are getting better and more credible and using deepfake to impersonate close friend of victim could be next step how to improve it, if it is not already happening.

Creating "fake news" to influence a large audience is the most common use case of deepfakes because we live in an information era. There are many targets of "fake news" such as rigging elections, demoralizing military units, or manipulating the stock market. In this case, politicians, celebrities, and significant personalities will be used in deepfakes to influence audience. We can only imagine what one person or high quality deepfake can change with enough media reach. For example, after one tweet from Elon Musk about Tesla's stock, sends shares down more than 10 % almost immediately [14]. [6]

A real example of deepfake is famous video with Barak Obama insulting Donald Trump, which should spread awareness regarding the fast developing category of new thread [1]. Several years later another video stating Volodimir Zelenskyj talking about surrendering, it was proved that it is a manipulated video, and its purpose was to demoralize Ukraine army and make them capitulate [2].

Another field where deepfakes could be used is to tricky biometrics systems in which the attacker is a different person to the gain access (banking, building, ...) [5], to secured equipment, etc. It was proven that biometrics system is not ready to deal with deepfakes, and it will probably require to add a new module to authentication pipeline which will be detecting deepfakes [7]. Face or voice biometrics recognition systems are in greatest danger. The falsification of documents is related to this topic and there was a case of smuggling people across borders with an official passport containing morphed photos of two individuals [13].

These cases are only the tip of the iceberg, and in the future, everyone should ask if video on social media with film celebrity is real or even worse, if the evidence in courts is trustworthy or not. The solution for this is using tools capable of detecting deepfakes. Those tools have to be created with caution for unskilled users.

2.3 Types of deepfakes and their creation process

There are plenty of methods on how to create deepfakes, and as its name suggests some of them are based on deep neural networks, but not exclusively. This section describes most common types of learning networks used for creating image/video or voice deepfakes. One of the most popular types for face deepfakes is Generative adversarial network (GAN), and it is used to create completely new faces or face manipulations.

Each method leaves traces in the medium that can then be detected. This is one way to recognize deepfakes so understanding process of creation is an advantage. Detecting will be described in more detail in Chapter 3.

2.3.1 Neural networks

All the facts regarding neural networks were retrieved from [11]. Neural networks are composited from neurons arranged in layers, and each layer is connected sequentially via synapses. Synapses are weighed, and the process of finding the proper value of all weights is called a learning neural network. To obtain results from the input of n-dimensional x process `forward-propagation` is used to propagate x through each layer.

Input to layer is vector a of values calculated by previous layer or in case of first layer x itself. That means result of each layer is also vector calculated by activation function $f(a * W + b)$, where f is activation function (Sigmod, ReLU, etc.), a is input vector, W is matrix of weights between layers i and $i + 1$ and b is dimensional bias. Dimensional bias is a constant offset that helps the network shift the activation function toward the positive or negative side [1].

[1] https://www.buzzfeed.com/craigsilverman/obama-jordan-peele-deepfake-video-debunk-buzzfeed

[2] https://www.youtube.com/watch?v=X17yrEV5sl4

Now let's consider the neural network M as a black box and denote its execution as $M(x) = y$. Supervise learning to train M is using paired samples with from (x_i, y_i) and loss function L is defined. Loss function is to generate a signal at the output of M and propagate him back to find error of each weight in synapses.

Optimalization algorithms such as gradient descent are then used to calculate new weights of M for the number of epochs. As a result of this process, the network learns the function $M(x_i) \approx y_i$ and is capable of making prediction on unseen data. More detailed descriptions of this could be found in the work of Y. Mirsky and W. Lee [11].

Next list shows types of neural networks used for generating deepfakes [11]:

- Generative Adversarial Networks (GAN) – Consist of two neural networks working against each other. One layer is generator and second is discriminator. Generator producing fake features trying to fool discriminator, on the other hand, discriminator is learning to distinguish between real sample and fake one.

- Encoder-Decoder networks (ED) – Contains at least two networks, encoder and decoder. It has narrowed layers towards its center. If encoder En and decoder De are symmetric and they are trained as $De(En(x)) = x$, then the network is called autoencoder. Generating deepfakes using ED trained with function $De(En(x)) = x_g$, where x_g is fake generated features. There is possibility to use multiple different ED chained after each other or using specific variant of ED called variational autoencoder.

- Convolutional Neural Network (CNN) – CNN is learning pattern hierarchies in the data. For deepfakes purposes, it learns filters applied over the input and forming an abstract feature map as the output.

- Recurrent Neural Networks (RNN) – RNN can handle variable length data and it is remembering stat after processing which can be used in next iteration. RNN are mostly used in audio.

Each architecture has its own subcategories that have small modifications or using some techniques from different architecture. All above mentioned neural networks types are shown in 2.2 and 2.3

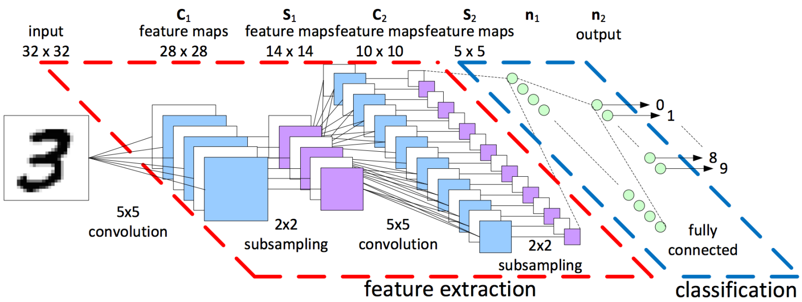


Figure 2.2: Architecture of convolutional neural network. Retrieved from [3].

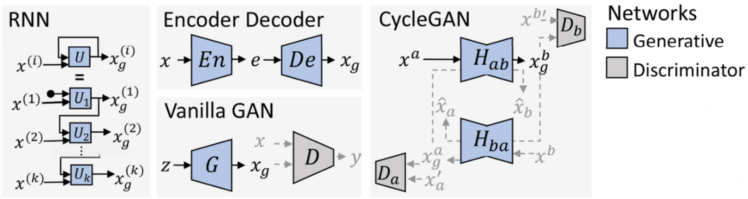


Figure 2.3: Basic neural network architectures (RNN, ED, GAN). Retrieved from [11].

2.3.2 Voice deepfakes

Speech synthesis is divided into two categories based on input data. Text to speech (TTS) converts written text to artificial speech and second category is called voice conversion (VC). The voice conversion consumes source voice, and both methods produce synthesis voice saying desired phrases specified by the input. [4]

Voice deepfakes are used independently or with deepfake video (e.g. full puppet). Creating synthesis voice is computationally challenging and one of the goals is making real-time voice conversion. There are several projects that are trying to accomplish this [3] [4].

2.3.3 Image or video deepfakes

The list of the following deepfakes is based on the work R. Tolosana, et al. [8]:

- Identity swap – Replacing the face of subject with the face of target as shown in Fig. 2.4. There are two different approaches, classical computer graphics-based technique and deep learning technique. Generally, the process of swap could be described as face detection, cropping, extraction of intermediate representations, synthesis of new face, and blending the generated face.

Figure 2.4: Examples of real and fake identity swap images. Retrieved from [8].

[3] https://github.com/SolomidHero/real-time-voice-conversion
[4] https://www.resemble.ai/speech-to-speech/

- Full puppet – Method related to identity swap allows creation of so-called puppet. One person (master) is source of facial expression and body movements that are mapped onto target person as shown in Fig. 2.5. [6]

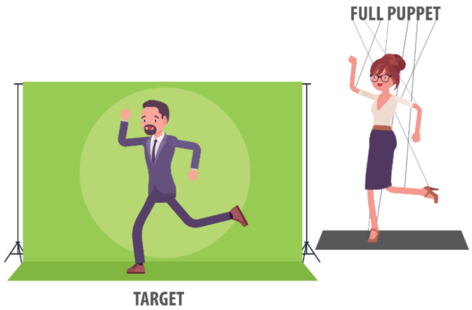


Figure 2.5: Full puppet technique visualisation. Retrieved from [9].

- Morphing – It is a type of manipulation that is used to create artificial biometric face samples. Final face contains resemble biometric information of two or more individuals. It should be possible to be successfully verified by biometrics systems for all individuals who were source for given deepfake. Fig. 2.6 shows an example of a morphed image.

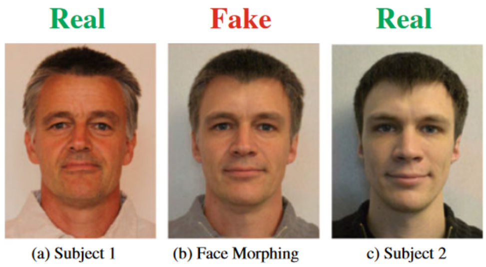


Figure 2.6: Examples of fake morphed identity from Subject 1 and Subject 2. Retrieved from [8].

- Attribute manipulation – Face editing or face retouching technique involves modifying some attributes such as length or color of hair, color of skin, sex, age, adding glasses or other artefacts, and more. Fig. 2.7 shows an example of this technique.

Figure 2.7: Examples of real and fake attribute manipulation category. Retrieved from [8].

- Expression swap – Modifying facial expression of the subject as shown in Fig. 2.8. This technique is used as one of part for full puppet.

Figure 2.8: Examples of real and fake expression swap category. Retrieved from [8].

- Audio/text to video – This method related to expression swap synthesising facial expression from audio or text. It is also known as lip-sync deepfakes. Diagram in Fig. 2.9 shows how this method works.

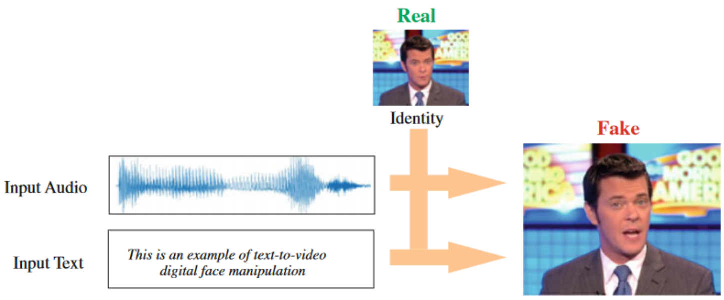


Figure 2.9: Examples of real and fake audio/text to video fake category. Retrieved from [8].

Creating deepfakes nowadays is complex task and many deepfakes is using more techniques so that they could be included into more than one category. Attackers could create deepfake that will fall under identity swap category and after that use attribute manipulation to tune final results.

Chapter 3

Deepfake detection

As we stated humans are not good in recognizing deepfakes. Creating deepfakes could leave visible defects (e.g. blurring or misalignment on edges in image). A. Firc summarize list of features to focus on while spotting fakes for humans [4].

- Facial features – eyes and their movement, eyebrows, glasses, facial expression, hair and facial hair, skin, lips, teeth
- Body features – body position and posture, body movements
- Voice features – unusual tempo, end of words, fricatives, conversation
- General indices - blurring or misalignment on edges, inconsistence noise or audio

This list pointing to most critical parts of deepfakes where some defects could be spotted created by creation process. Generation of deepfakes are getting better and other masking techniques are used. Huge problem for deepfake detection is lossless compression, several chained resize of image, application of noise etc. Basically, all method that led to some data loss but still maintained main information, means no notable change for naked eye or ear. Manual post processing could be used for polishing results (images – Photoshop, GIMP; etc) when previous methods are still not good enough.

Machine detection could be divided into two categories, standard algorithms looking for physical inconsistency, digital integrity, using same features as A. Firc described. Other methods are based on machine learning. Same "masking" techniques listed before have a same effect for machine based detection because there is data loss, preventing usage of reliable methods like frequency analysis. Still computers perform better than humans, because they can also use different features (e.g. pixel level features), especially neural networks trained for deepfake detection. In case where we are not looking only for deepfakes but we expend input set to all synthetic media we can use similar methods. Difference will be in learning process (training data) or features selection. Worst case scenario is only recognizing suspicious images containing traces after possible masking techniques such as double compression traces, noise patterns, etc. [15]

Another problem of detection algorithms is bad generalization. Most of methods are trained on single domain deepfake (e.g. identity swap) that means they are not able recognize deepfake from different category. When methods are trained on multi domain datasets accuracy is going down. [10]

3.1 Image/Video detection methods

As stated, before most of methods for deepfake detection is targeting only single domain. This section will describe examples of proposed detection methods for image/video deepfakes. There are more conventional approaches and also more "exotic".

P. Majumdar, et al. referring to multiple detection methods for image retouching (makeup, filters) and alternation (fully synthetize faces, morphing) [10]. Most of them use same pattern which could be described as specific feature extraction followed by support vector machines (SVM) for classification. One of methods proposed detection of images using face patches as input in the deep Boltzmann machine for feature extraction and SVM for binary classification. Another method uses softmax probabilities as the features in the SVM. Other methods for example using convolutional neural networks. [10]

L. Spreeiwers, et al. made research on using local binary pattern with SVM for morphing detection [?]. A single LBP histogram contains 59 feature values, which means for a 3×3 layout the feature space has 531 dimensions. The SVM classifiers are trained on between 650 and 1,000 samples. They also stated that EER increase to above 20

Non-conventional detection method is heart rate estimation (remote photoplethysmography) by J. Fierret [?]. They are trying to estimate hearth rate from video and evaluating frame by frame. There are other human physiological processes that could be used instead heart rate such as blood oxygen or breath rate. Score is oscillating during the video and final decision is based on mean/median/QCD score.

There are many other methods, and each will have its pros and cons but as we can observe SVM classification with large range of different feature extractors. Other rising group of detectors is using CNN. There are not many researches using CNN as SVM but results seems to be promising as we can see in reaeches [?] [?].

3.2 Voice detection methods

Voice detection complicates different languages, it is similar story to image/video deepfakes. There are face swaps, morphing, etc. and for voice there are different languages and dialects. Voice detection methods also coping trend from image/video detection methods. SVM with differete feature extractors or CNNs.

Z. Almutairi and H. Elgibreen referring multiple methods. One of them using SVM model with Random Forest (RF) to predict synthetic voices based on a feature called Short-Term Long-Term. In this research they compared SVM with many other classifiers such as Linear Discriminant, Quadratic Discriminant, Linear SVM, weighted K-Nearest Neighbors (KNN) and SVM outperforms all of them. Other referred work using combination of two CNN, 1-D CNN and Siamese CNN. The Siamese CNN contained two identical CNNs that were the same as the 1-D CNN but concatenated them using a fully connected layer with a softmax output layer. Input to 1-D CNN was the speech log-probabilities. [?]

3.3 Analysis of existing tools for detecting deepfakes

3.3.1 Deepware

- https://scanner.deepware.ai/developer/

3.3.2 Deepstar

- https://www.zerofox.com/deepstar-open-source-toolkit/

3.3.3 Sensity

- https://sensity.ai/deepfakes-detection/

Chapter 4

Architecture and technologies analysis

4.1 Requirements

Functional requirements:

- možnost přidat, odebrat metodu
- více detekčních metod naráz
- možnost změnit model metody (přetrénovaný model na jinou datovou sadou)
  - požadavky na vstupní formát dat zaobaluje detekční metoda
- nahrání fotky, videa, audio nahrávky
  - base line - soubor, link
  - chtěné rozšíření - element stránky
- srozumitelná reprezentace výsledků (široká veřejnost)
- security (kontrola vstupních dat, zahlcení)
- sběr statistik
  - analýza jaká data je možné ukládat (privacy policy)
- sběr feedbacku

Non-functional requirements

- škálovatelnost (jednotky až tisíce uživatelů)
- krátká doba odezvy (jednotky, malé desítky sekund)
- low cost provoz (cloud -> cena za výpočetní čas)
- co nejvetší přenositelnost mezi různými prohlížeči
- open-source

4.2 Containerazation

- docekr, docker-compose, kubernetes, podman, LXC

4.3 Web server

- python, c#, ...

4.4 Web browser plugin

- html, css, typesctipt, ...

Chapter 5

Framework architecture

5.1 Containerazation and scaling

5.2 High level architecture

https://microservices.io/patterns/microservices.html

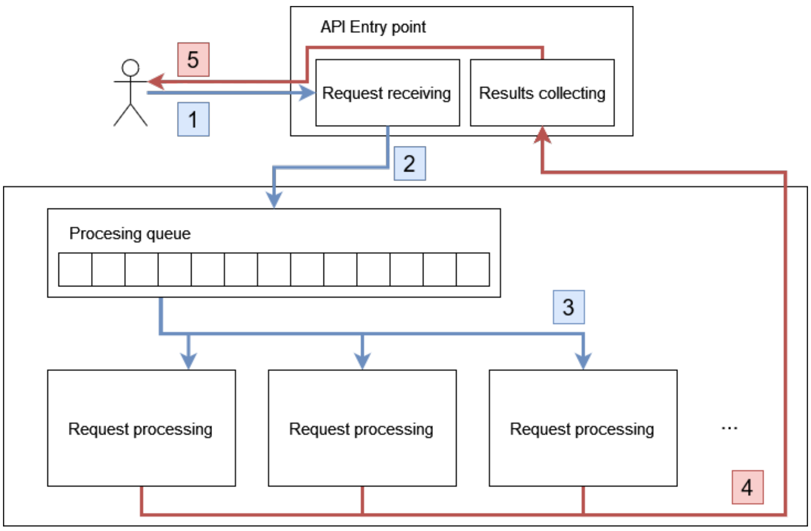


Figure 5.1: ...

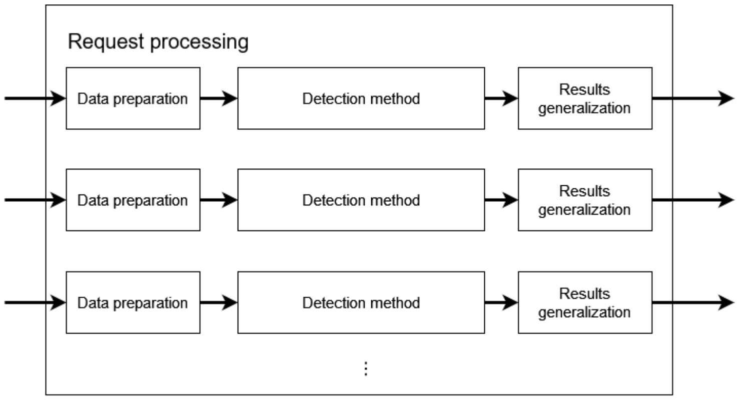


Figure 5.2: ...

- /ping
  - GET /ping – healtcheck
- /detect
  - POST /detect/file – ...
  - POST /detect/link – ...
- /progress
  - GET /progress/<request_id> – websocket

5.3 Input layer

5.4 Request processing

5.4.1 Data preparation layer

5.4.2 Inividual detection method

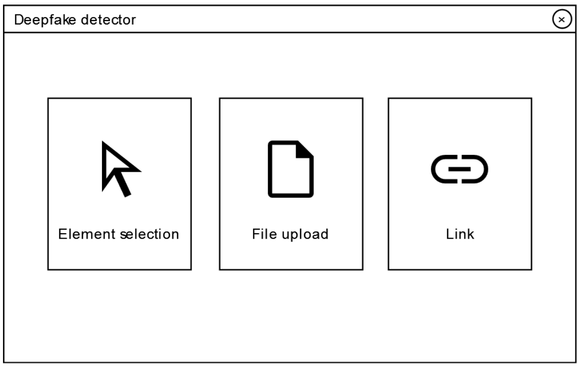
5.4.3 Results generalization

5.5 Output layer

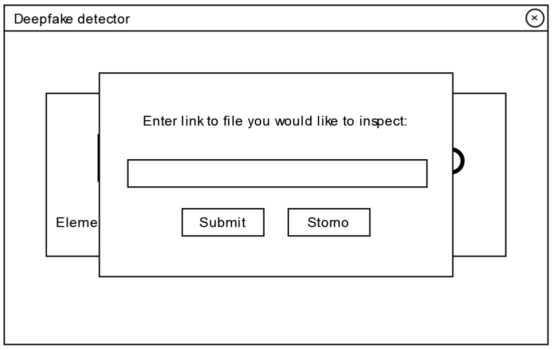
Chapter 6

Client architecture

6.1 Web browser plugin

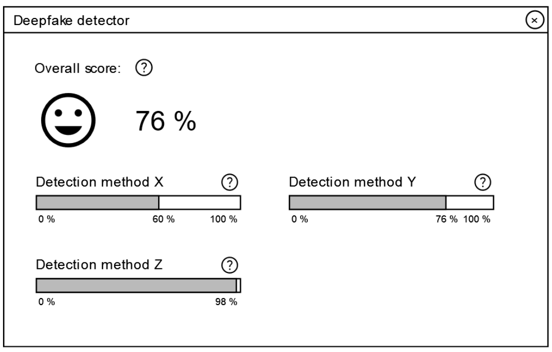


(a) ...

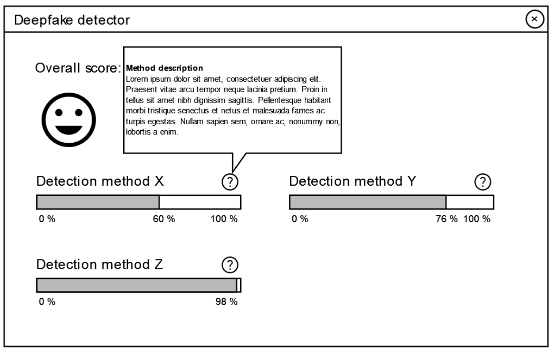


(b) ...

Figure 6.1: ...



(a) ...



(b) ...

Figure 6.2: ...

Figure 6.3: ...

Chapter 7

Conclusion

Bibliography

[1] *What Is the Necessity of Bias in Neural Networks?* [https://www.turing.com/kb/necessity-of-bias-in-neural-networks]. [cit. 2022-12-29].

[2] Amos, Zachary. *Hybrid Vishing Attacks Skyrocketing: What to Know* [https://itsupplychain.com/hybrid-vishing-attacks-skyrocketing-what-to-know/]. 2022 [cit. 2022-12-28].

[3] Deotte, C. *How to choose CNN Architecture MNIST* [https://www.kaggle.com/code/cdeotte/how-to-choose-cnn-architecture-mnist]. [cit. 2023-01-04].

[4] Firc, A. *Applicability of Deepfakes in the Field of Cyber Security*. Brno, CZ, 2021. Diplomová práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Available at: https://www.fit.vut.cz/study/thesis/23761/.

[5] Firc, A. and Malinka, K. The dawn of a text-dependent society: deepfakes as a threat to speech verification systems. In: *SAC '22: Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing*. Association for Computing Machinery, 2022, p. 1646–1655. DOI: 10.1145/3477314.3507013. Available at: https://www.fit.vut.cz/research/publication/12595.

[6] Homeland Security. *Increasing Threat of Deepfake Identites* [https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf]. 2021 [cit. 2022-12-16].

[7] Ibsen, M., Rathgeb, C., Fischer, D., Drozdowski, P. and Busch, C. Digital Face Manipulation in Biometric Systems. In: *Handbook of Digital Face Manipulation and Detection: From DeepFakes to Morphing Attacks*. Springer International Publishing, 2022, p. 27–43. DOI: 10.1007/978-3-030-87664-7_5. ISBN 978-3-030-87664-7. Available at: https://doi.org/10.1007/978-3-030-87664-7_5.

[8] Ibsen, M., Rathgeb, C., Fischer, D., Drozdowski, P. and Busch, C. An Introduction to Digital Face Manipulation. In: *Handbook of Digital Face Manipulation and Detection: From DeepFakes to Morphing Attacks*. Springer International Publishing, 2022, p. 3–26. DOI: 10.1007/978-3-030-87664-7_5. ISBN 978-3-030-87664-7. Available at: https://doi.org/10.1007/978-3-030-87664-7_5.

[9] Korshunov, P. and Marcel, S. The Threat of Deepfakes to Computer and Human Visions. In: *Handbook of Digital Face Manipulation and Detection: From DeepFakes to Morphing Attacks*. Springer International Publishing, 2022, p. 97–115. DOI:

10.1007/978-3-030-87664-7_5. ISBN 978-3-030-87664-7. Available at:
https://doi.org/10.1007/978-3-030-87664-7_5.

[10] Majumdar, P., Agarwal, A., Vatsa, M. and Singh, R. Facial retouching and alteration detection. In: *Handbook of Digital Face Manipulation and Detection: From DeepFakes to Morphing Attacks*. Springer International Publishing, 2022, p. 367–387. DOI: 10.1007/978-3-030-87664-7_5. ISBN 978-3-030-87664-7. Available at:
https://doi.org/10.1007/978-3-030-87664-7_5.

[11] Mirsky, Y. and Lee, W. The Creation and Detection of Deepfakes: A Survey. *ACM Comput. Surv.* New York, NY, USA: Association for Computing Machinery. 2021, vol. 54, no. 1. DOI: 10.1145/3425780. ISSN 0360-0300. Available at:
https://doi.org/10.1145/3425780.

[12] Müller, N. M., Pizzi, K. and Williams, J. Human perception of audio deepfakes. In: *Proceedings of the 1st International Workshop on Deepfake Detection for Audio Multimedia*. Association for Computing Machinery, 2022, p. 85–91. DOI: 10.1145/3552466.3556531. ISBN 9781450394963. Available at:
https://doi.org/10.1145/3552466.3556531.

[13] Scherhag, U., Rathgeb, C. and Busch, C. Face Morphing Attack Detection Methods. In: *Handbook of Digital Face Manipulation and Detection: From DeepFakes to Morphing Attacks*. Springer International Publishing, 2022, p. 331–349. DOI: 10.1007/978-3-030-87664-7_5. ISBN 978-3-030-87664-7. Available at:
https://doi.org/10.1007/978-3-030-87664-7_5.

[14] Shead, S. *Elon Musk's tweets are moving markets — and some investors are worried* [https://www.cnbc.com/2021/01/29/elon-musks-tweets-are-moving-markets.html]. 2021 [cit. 2022-12-28].

[15] Verdoliva, L. Media Forensics and DeepFakes: An Overview. *IEEE Journal of Selected Topics in Signal Processing*. 2020, vol. 14, no. 5, p. 910–932. DOI: 10.1109/JSTSP.2020.3002101.