BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Excel@FIT 2023

Deepfake Detection Framework

Bc. Jan Bernard, xberna18@stud.fit.vutbr.cz
Supervisor: Mgr. Kamil Malinka, Ph.D.

a.k.a (DF)^2

Motivation

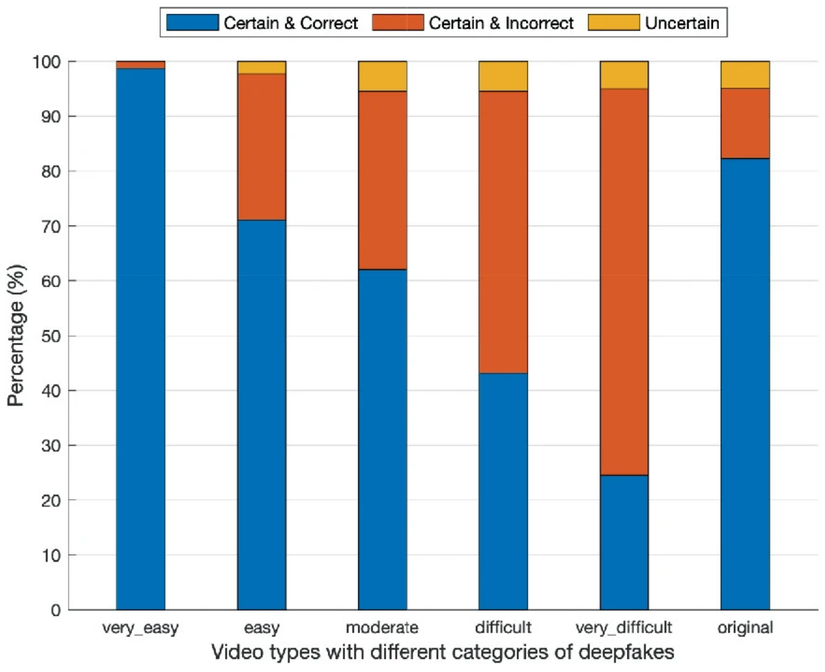

Figure 1: Subjective answers from ANOVA test for different deepfake categories. Retrieved from [1]

Diffret types of deepfakes

- Audio
- Image
- Video

Figure 2.1: Examples of real and fake attribute manipulation category. Retrieved from [2].

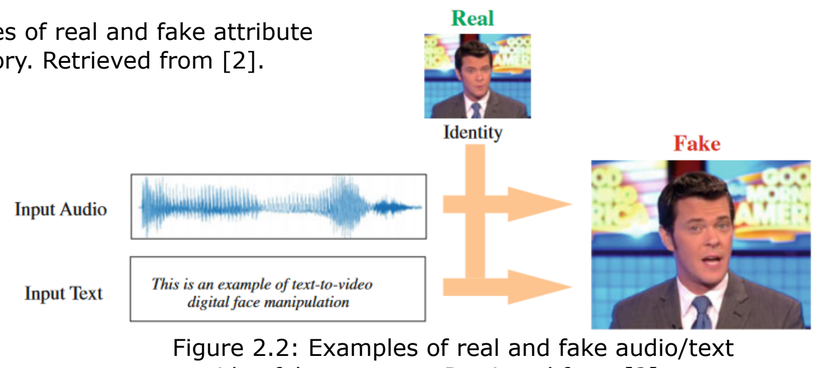

Figure 2.2: Examples of real and fake audio/text to video fake category. Retrieved from [2]

Detection framework

Architecture

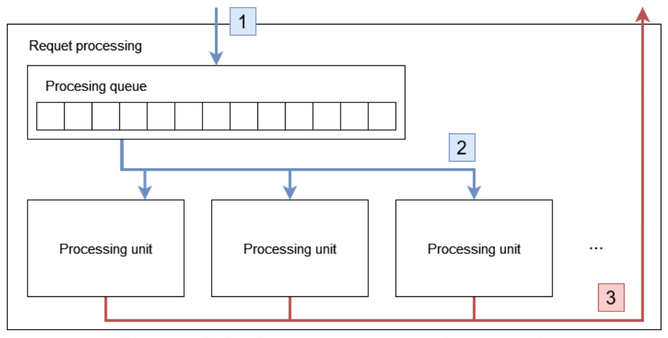

Figure 3.2: Request processing detail

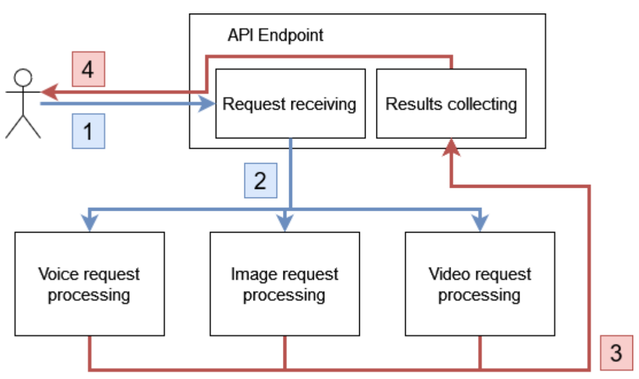

Figure 3.1: High-level design of whole framework

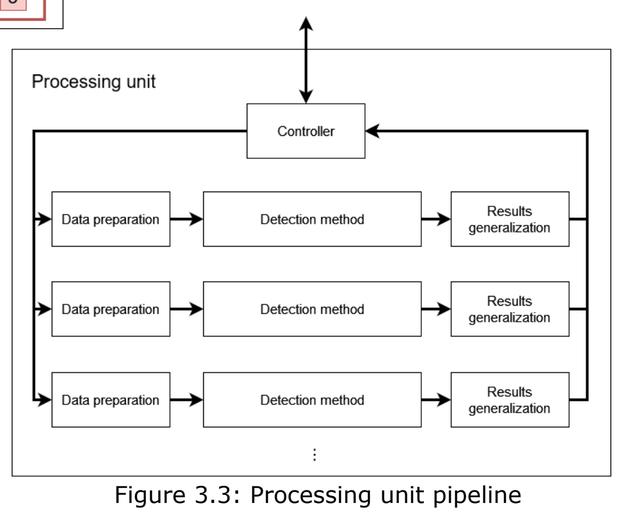

Figure 3.3: Processing unit pipeline

Implementation

- C#
- RabbitMQ
- Python + FastAPI
- MSSQL
- Kubernetes
- Docker
- Prometheus
- Grafana

and more...

Client application

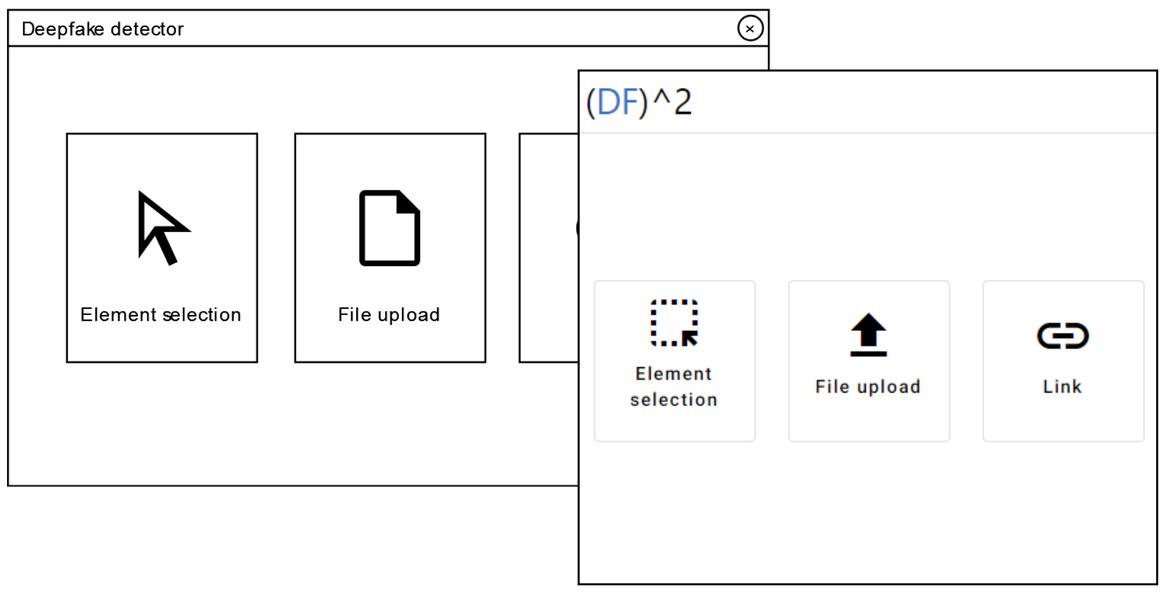

Figure 5.1: Input type selection screens

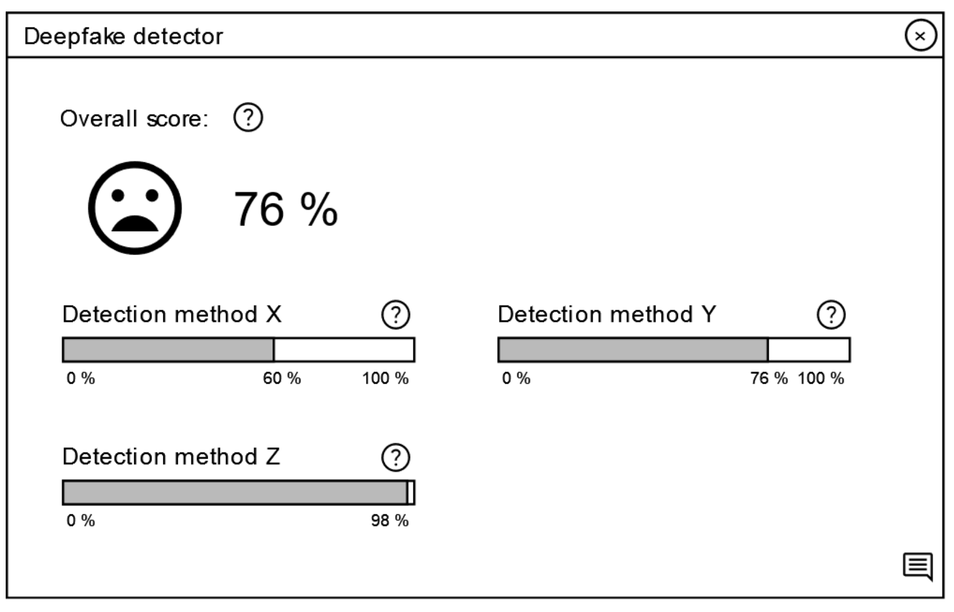

Figure 5.2: Results view screen

References

[1] 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.

[2] 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.