Testing the Robustness of a Voice Biometrics System against Deepfakes

2023

Author: *Bc. Jakub Reš*
Supervisor: *Mgr. Kamil Malinka Ph.D.*

Motivation

- Deepfakes – DNN forgeries
- Standards – practices for testing using conventinal sources of spoofs
- Deepfakes need more attention
- Lack of generic methodologies

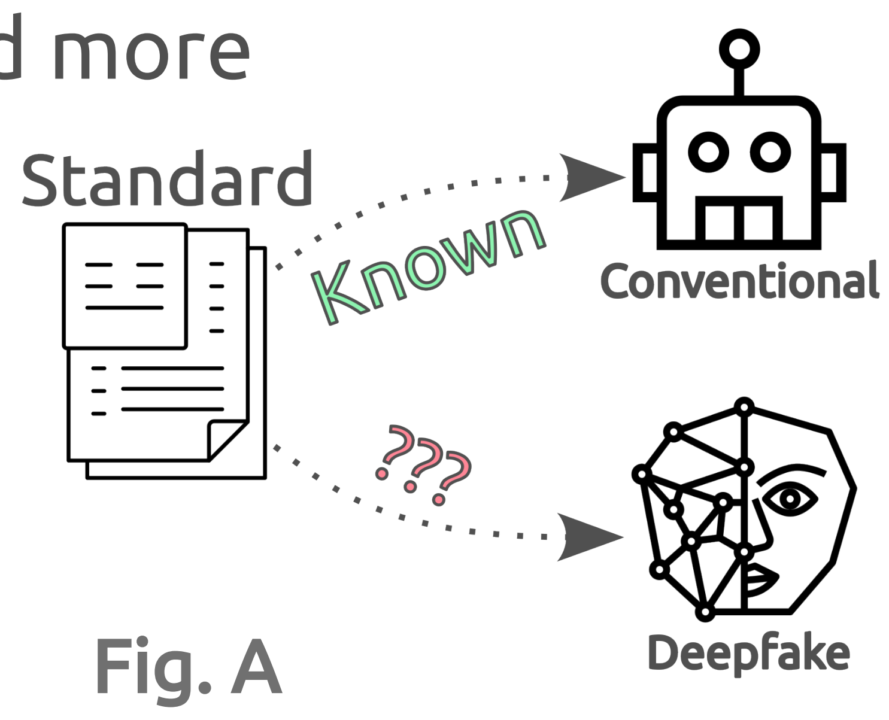

Fig. A

Test execution report

- Environment
- Biometric system properties
- Communication
- Experiments
  - Scenario fulfilment
  - Data usage
  - Results
- Evaluation

System ID	AUC	Eval
A01	1,0	OK
A08	1,0	OK
A10	0,91	?
A12	0,99	OK
A15	0,99	OK

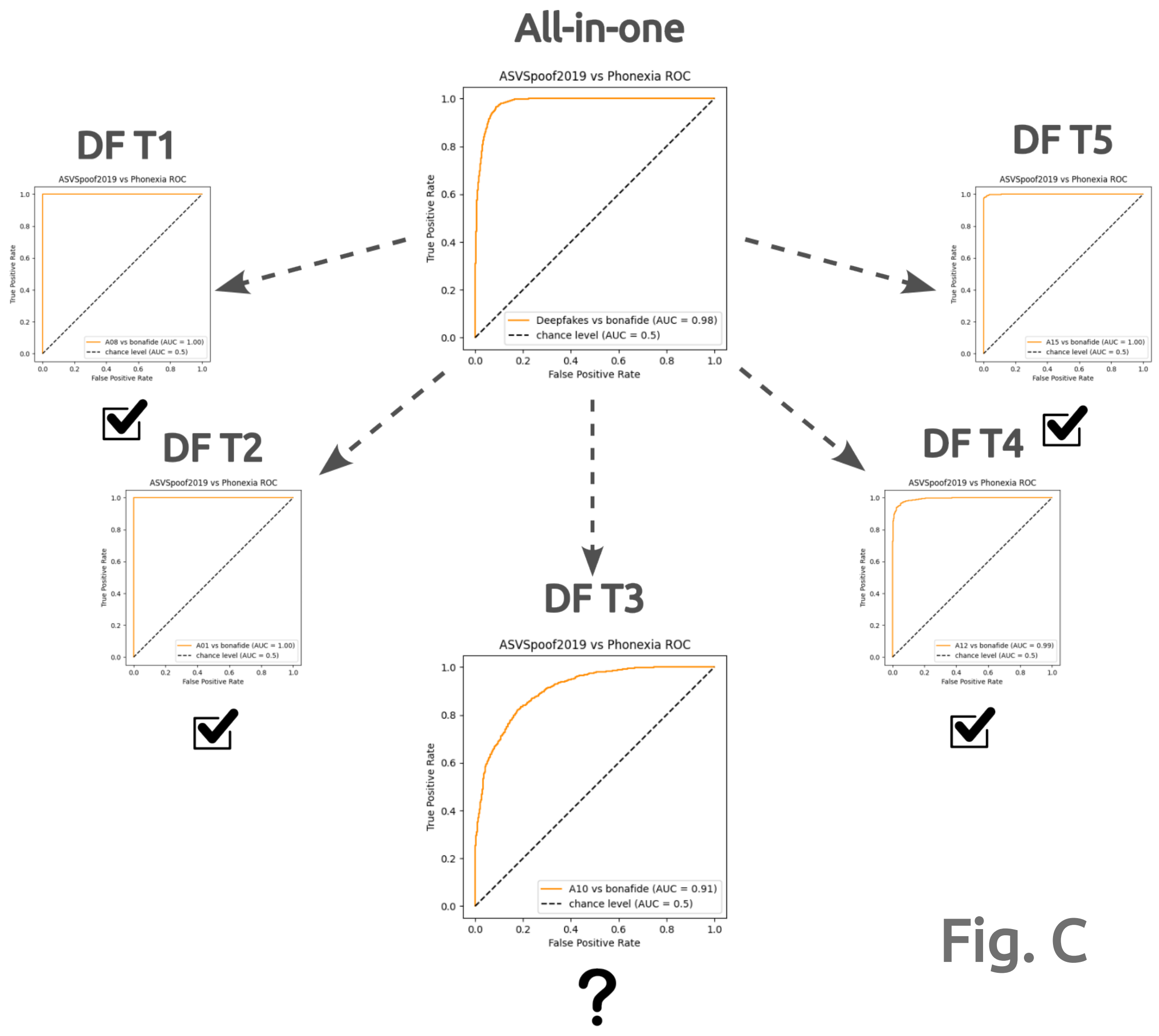

Fig. C

Testing method

- Specific method
  - Goal – different types of deepfakes
  - Use-case – voice-as-a-password
  - Attacker model -
    - Motive - money/fame
    - Means – tools
    - Opportunity – access
  - Scenario
  - Dataset – public
  - Metrics – standard + custom

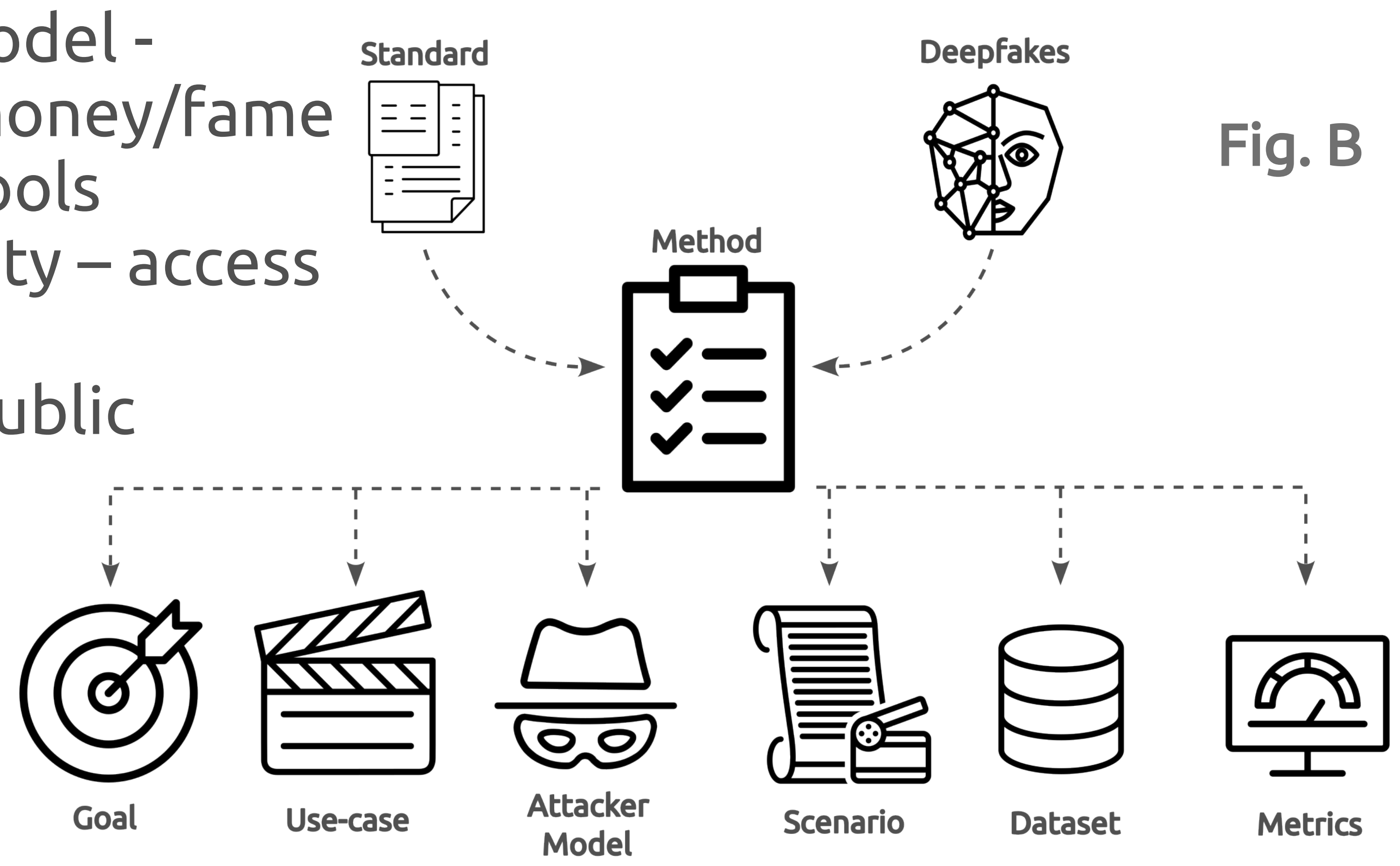

Fig. B

Methodology

- Repeatable procudere based on proven practices
- Recommendations and suggestions
- Five main areas:
  - Planning – planing the test (Fig. B)
  - Acquiring the dataset – public/custom
  - Conducting the test
  - Evaluation – metric options
  - Interpretation – relevance of results

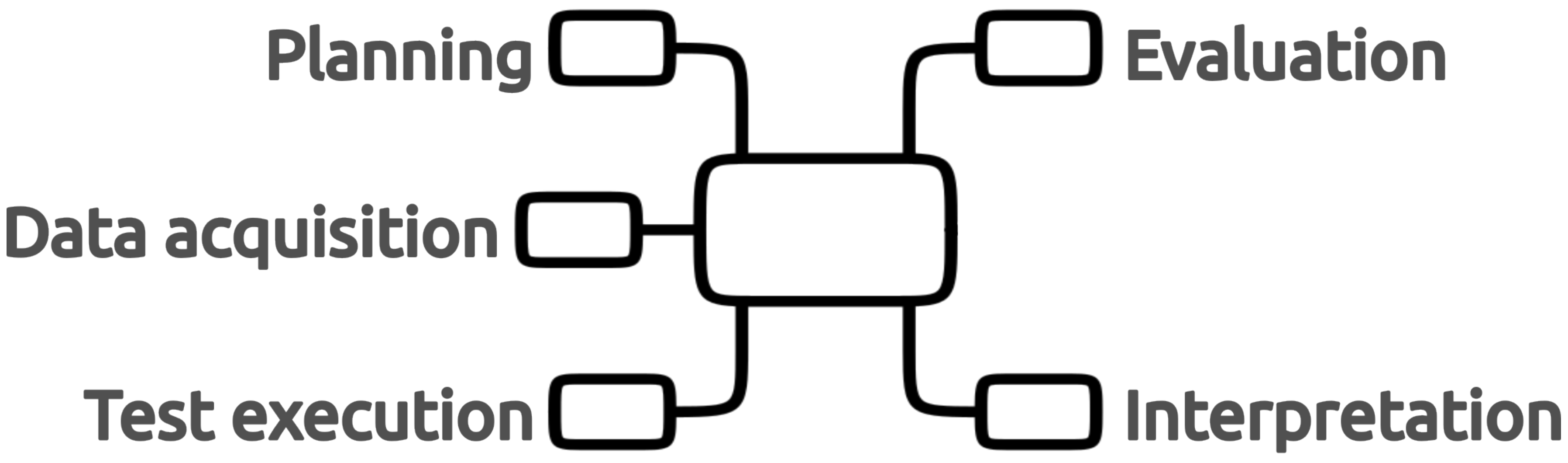

Fig. D

Excel@FIT 2023

BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY