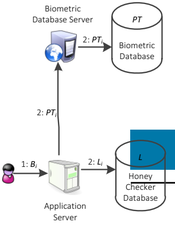


Biometric Template Protection

A honey-based approach

NTNU

Motivation

- Biometrics are highly sensitive personal data and any information leakage poses severe security and privacy risks. Biometric templates should hence be protected and impersonation with stolen templates must be prevented, while preserving the system's performance.
- Most existing biometric template protection schemes do not provide as strong security as cryptographic tools.
- Furthermore, they are rarely able to detect during a verification process whether a template has been leaked from the database or not.

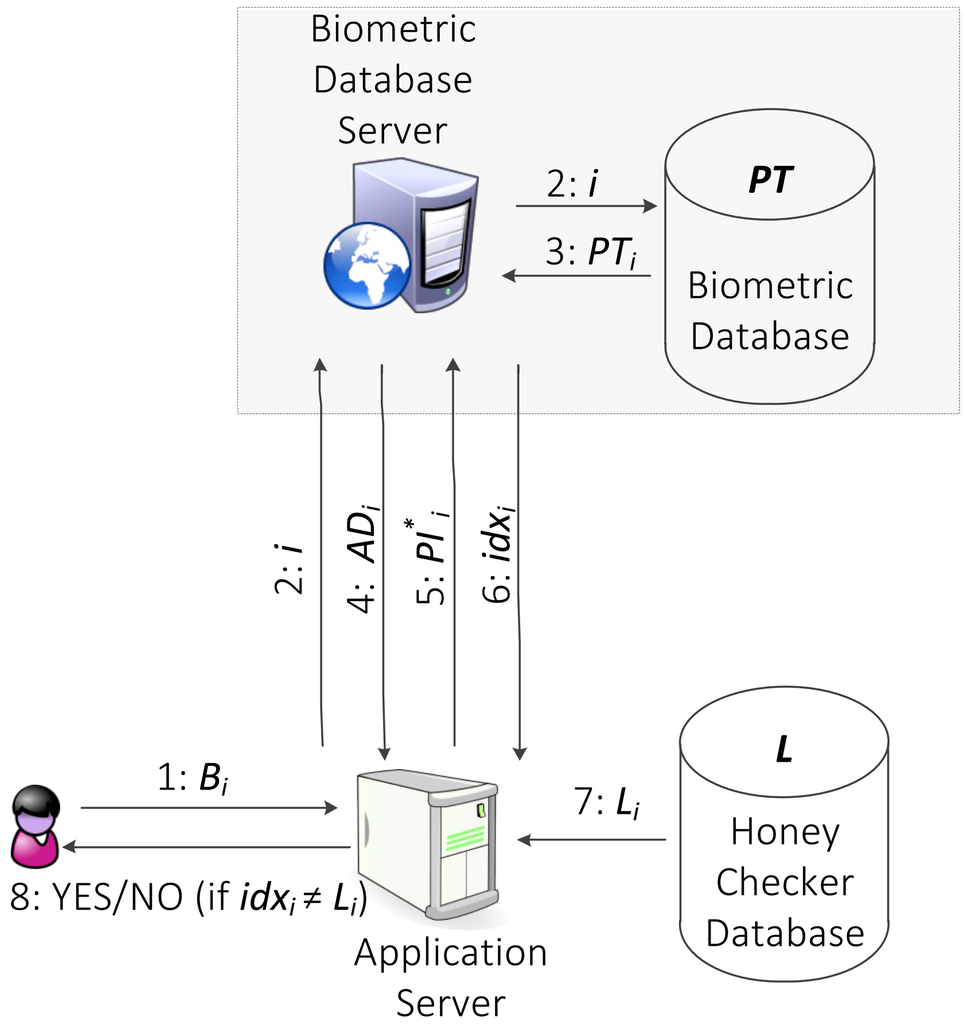
Objectives

- Generate indistinguishable synthetic templates for different biometric characteristics.
- Design secure algorithms for template protection, and their integration within the honey-based framework.
- Create fusion schemes under a multimodal system, whose products are compact and reliable *honey* and real templates.

Approach

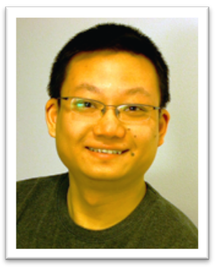
- In our work we suggest a two-level security at template level, which consist of: template protection mechanisms design, and the generation of indistinguishable synthetic templates.
- Synthetic templates, named *honey templates*, are stored in the same storage space with the real template to camouflage it.
- During verification the system will compare the newly presented template with the whole set of templates. The best matched template index will be compared with the previously stored index in the Honey Checker Database. If they don't match the system will consider this attempt as information leakage.

Computation and database able to be outsourced



- *Fig. 1 Architecture design of the verification phase of a honey-based biometric system.*

Edlira Martiri
edlira.martiri2@ntnu.no



Dr. Bian Yang
bian.yang@ntnu.no

Prof. Dr. Christoph Busch
christoph.busch@ntnu.no

Norwegian University of Science and Technology – Norwegian Biometrics Lab