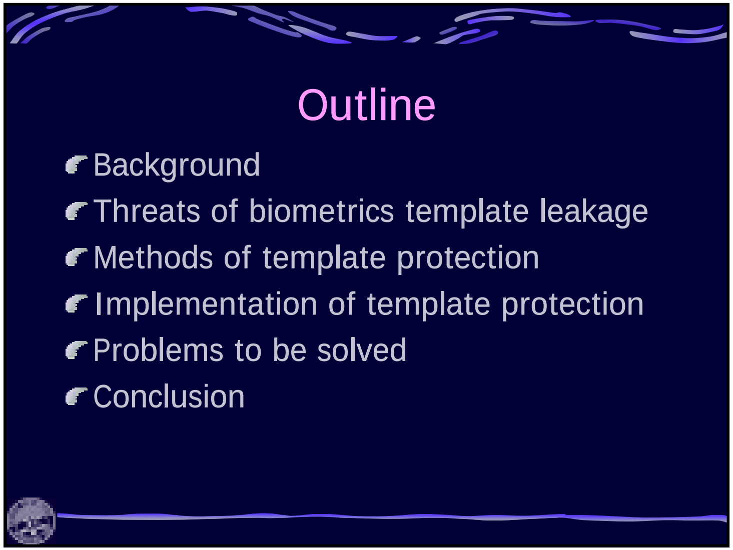
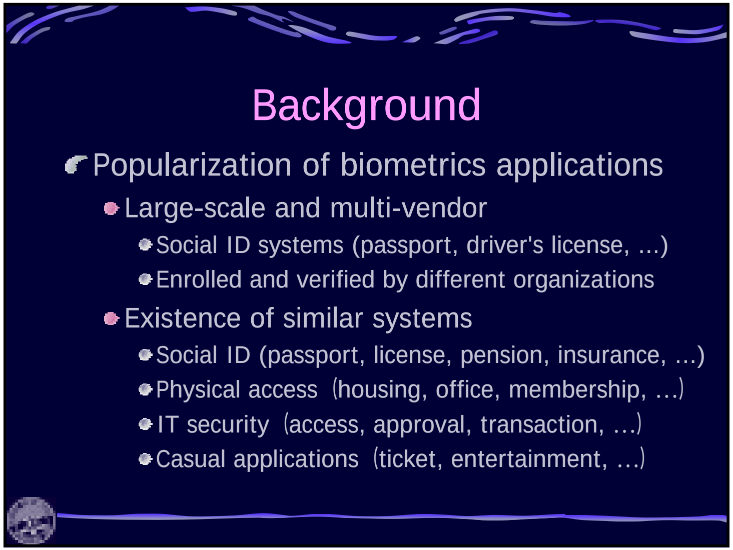
Privacy Protection for Biometrics Personal Authentication Systems

Kazuhiko Sumi
Graduate School of Informatics
Kyoto University



Outline

- Background
- Threats of biometrics template leakage
- Methods of template protection
- Implementation of template protection
- Problems to be solved
- Conclusion



Background

- Popularization of biometrics applications
  - Large-scale and multi-vendor
    - Social ID systems (passport, driver's license, …)
    - Enrolled and verified by different organizations
  - Existence of similar systems
    - Social ID (passport, license, pension, insurance, …)
    - Physical access（housing, office, membership, …）
    - IT security（access, approval, transaction, …）
    - Casual applications（ticket, entertainment, …）

Effect of Common Template

- Pros：
  - Standardized template is stable
  - Easy to design a new application
  - Certified template can be trusted
  - Operational cost reduction (no enrollment)
  - Global standard（ISO19794）
- Cons：
  - Possible template leakage
  - Easy reverse engineering
  - Weak countermeasure against template leakage

Outline

- Background
- Threats of biometrics template leakage
- Methods of template protection
- Implementa
- Problems t
- Conclusion

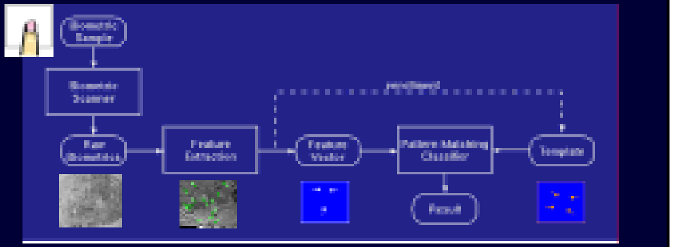
It is only one of the many threats in biometrics authentication systems.

However, template leakage is special to biometrics authentication. It is similar to secret key leakage but biometrics cannot be changed!

Special treatment is required for biometrics template protection.

Reference Model

- A biometrics authentication system extracts features from scanned biometrics and pattern matches it with enrolled template.

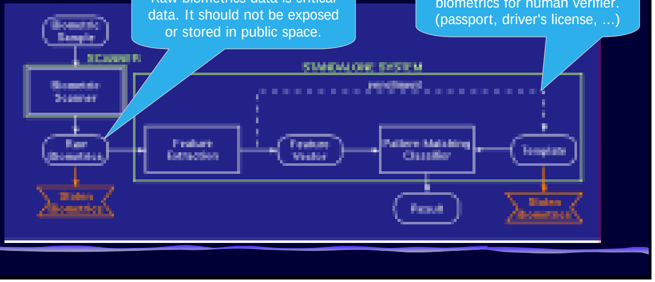


Vulnerability Caused by Template Leakage

- Leakage points
  - Raw sensor data
    - Tapping, Trojan horse
    - Template with raw biometrics
  - Encoded template in a working system
    - Center database
    - Device to center communication
    - Template in a device
    - Template in a token
  - Encoded template in a abandoned system
    - Template in a device

Leakage Scenario 1

- If the scanner output is tapped, or, if a template contains raw biometrics, raw biometrics data can be stolen.

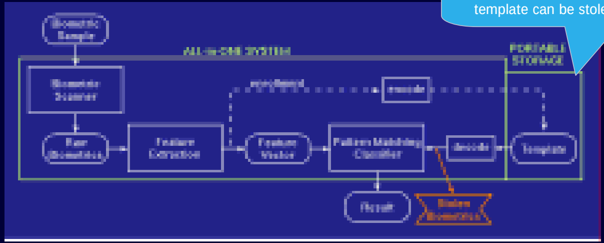


Raw biometrics data is critical data. It should not be exposed or stored in public space.

Some systems have raw biometrics for human verifier. (passport, driver's license, ...)

Leakage Scenario 2

- Even if a device has encrypted template, decrypted template can be tapped during authentication process.

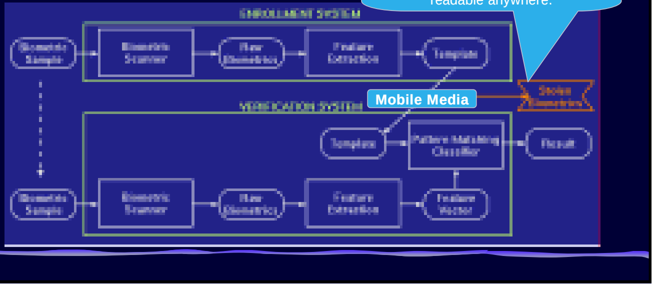


If the secret key to decrypt the template is stolen, the template can be stolen.

Leakage Scenario 3

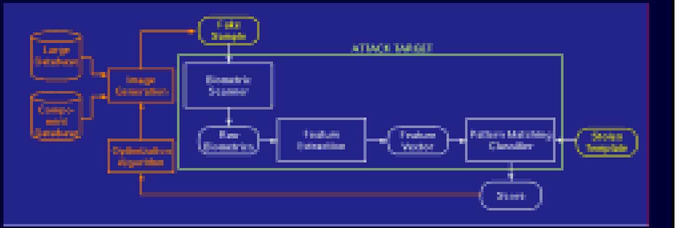
- Template can be stolen easily from interoperable systems with common template format and access key.

Coming IC Card passport has standardized template, which is readable anywhere.



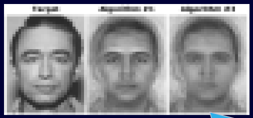
Is An Encoded Template Safe?

- Even if an attacked target is a black box, an effective template or raw biometrics can be generated by hill-climbing attack. (Adler,2003)



Template Recovery Examples

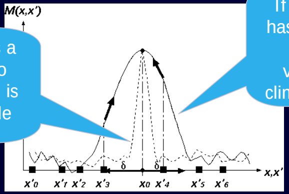
- From a set of image of different persons, a fake image, which is falsely accepted by a face authentication system, can be generated. (Adler,2003)



Take the closest samples as a starting point. Then, add a principle component in proportion to the similarity gradient on the component. After several times of iterations, the result can fool the authentication system.

Possibility of Hill-climb Attack

- Most of the biometrics authentication systems use a similarity score as an internal variable. If an enough number of starting points are given, it is possible to find the highest point without being trapped by local minima.



If the similarity score has a steep curve, it is safer to hill-climbing attack. But it is not robust against sample variations

If the similarity score has a broad curve, it is robust to sample variations. But hill-climbing attack is easy.

Outline

- Background
- Threats of biometrics template leakage
- Methods of template protection
- Implementation of template protection
- Problems to be solved
- Conclusion

Method of Template Protection

- Template access control
  - Store a template in a safe place.
- Encrypted template storage
  - Store an encrypted template, decrypt it on matching.
- Encrypted template
  - Matching is done in encrypted space.
- Cancelable template
  - Revoke the template if it is leaked.

SAFER

Template Encryption Technique

- Deformation / translation / block scramble
- Phase term in frequency domain
- Convolution / addition with random pattern
- Signal removal with error correction code

Deformation / Scramble

- Deform / transform an image or a template coordinate with a secret function.
- Apply the same deformation / transformation on verification.
- Pros: Matching function is backward compatible.
- Cons: Hill-climbing vulnerability remains.

Phase Term in Frequency Domain

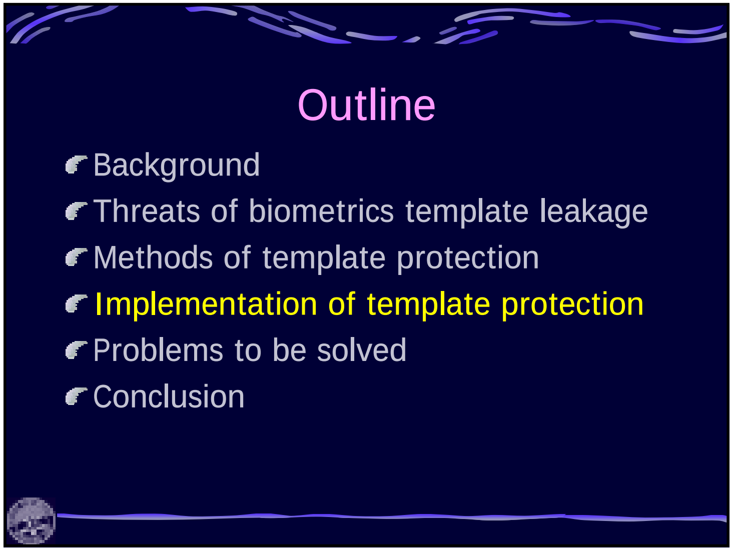
- Transform original biometric sample to frequency domain by FFT.
- Split off power-spectrum term. Store only phase-term in the template.
- Verification is done in frequency domain.
- Pros:
  - Very difficult to restore original signal.
  - Robust against hill-climb attack.
- Cons:
  - Less robust against small variation of a biometric sample.

Convolution / Addition With Random Patterns

- Matching is done with convolved templates. Convolved template and their matching scores are stored in template database.
- If matching scores are similar to those of original templates, similarity is guaranteed.
- Pros:
  - Very difficult to restore original signal.
  - Robust against hill-climb attack.
- Cons:
  - Less robust against small variation of samples.
  - Critical with number of patterns and trials.

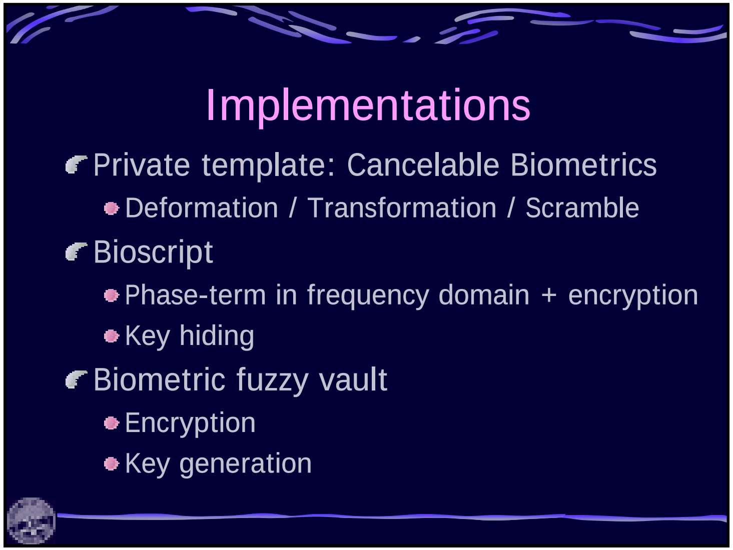
Signal Removal

- In addition to encrypted template, generate error correction code and remove the original signal.
- Removed signal is restored by error correction code.
- Pros:
  - Difficult to restore original signal.
- Cons:
  - Critical with error correction capability and actual recognition error.



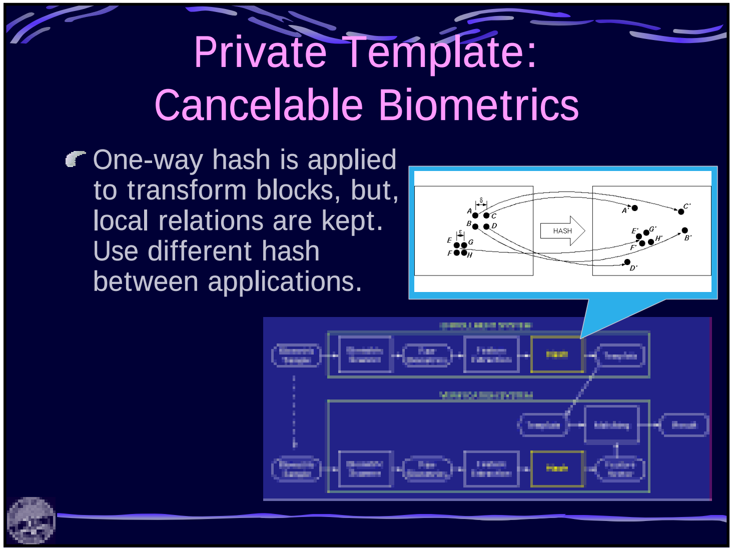
Outline

- Background
- Threats of biometrics template leakage
- Methods of template protection
- Implementation of template protection
- Problems to be solved
- Conclusion



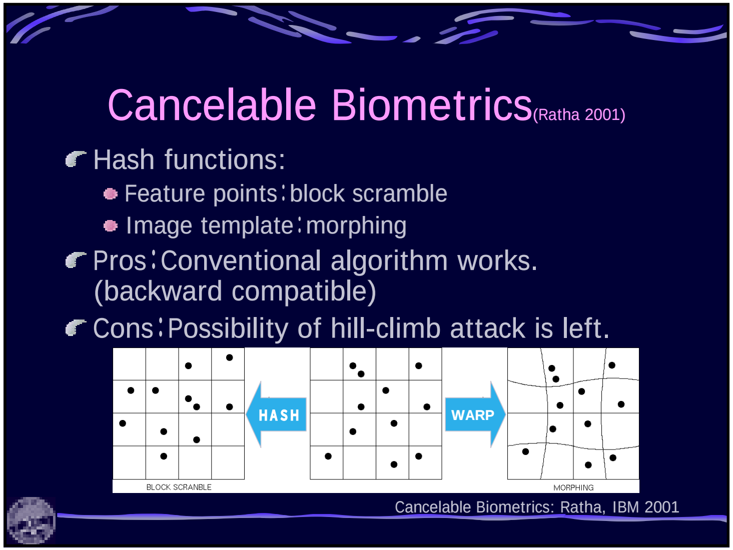
Implementations

- Private template: Cancelable Biometrics
  - Deformation / Transformation / Scramble
- Bioscript
  - Phase-term in frequency domain + encryption
  - Key hiding
- Biometric fuzzy vault
  - Encryption
  - Key generation



Private Template: Cancelable Biometrics

- One-way hash is applied to transform blocks, but, local relations are kept. Use different hash between applications.



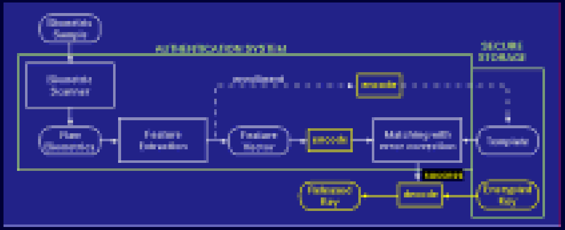
Cancelable Biometrics(Ratha 2001)

- Hash functions:
  - Feature points：block scramble
  - Image template：morphing
- Pros：Conventional algorithm works. (backward compatible)
- Cons：Possibility of hill-climb attack is left.

Cancelable Biometrics: Ratha, IBM 2001

Key Hiding and Retrieval

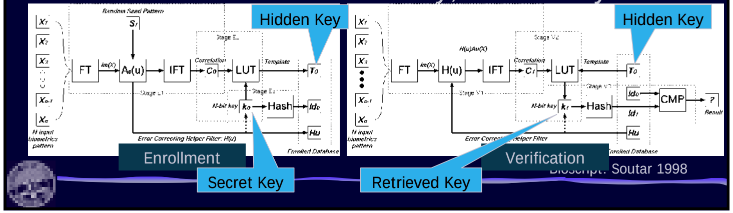
- The template is encoded with one-way hash function. If the matching is succeeded, secret key, which is transformed by hashed template is retrieved.



Bioscript: Soutar 1998

Bioscript(Soutar 1998)

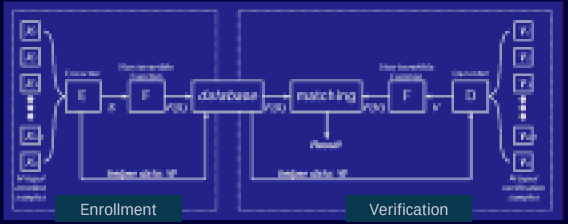
- Phase-term of Fourier transformed input fingerprint image and a random 2D pattern are convolved and error correction pattern and encoded secret key is stored in the template
- Pros: Cancelable, pattern shift tolerant.
- Cons: error-correction ability, hashed key exists.



Bioscript: Soutar 1998

Key Generation: general idea

- Hashed template F(S) and helper data W are stored. W restore the image Y, the they are matched in encrypted space. Matching result itself is the secret key.



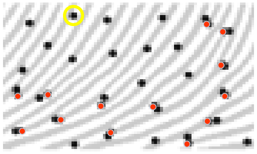
Linnartz and Tulys, Anonymous Biometrics, Phillips, 2003

Anonymous Biometrics (Linnartz, 2003)

- Helper data W may be:
  - Quantized Index Modulation
  - Error Correcting Code-scheme
  - Significant Components

Fingerprint Vault (Clancy 2003)

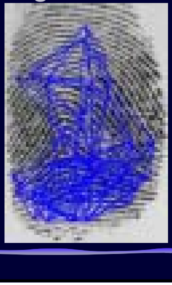
- Add random fake minutiae (chaff) to the original template. Bit width matching result is used as secret key.
- Pros: Secret key is not in the template.
- Cons: Pre-alignment is required. / Not robust against minutiae misdetection.

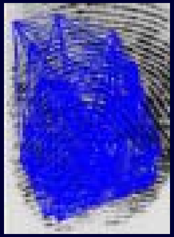


Clancy et al., UMD, 2003

Fingerprint Vault (Uldag 2003)

- Use pair of minutiae (line) instead of minutiae points
- Alignment capability





Uldag et al., MSU, 2003

Fingerprint Vault (Yang 2004)

- Use triples of minutiae instead of minutiae lines
- Better alignment capability

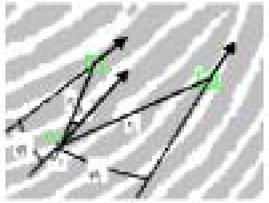


Fig. 2. Concept of the proposed feature

Yang, UCLA, 2004

Comparison of Key Generation Techniques

Paper Title and Author	Target	Alignment	Variation	Safety
Fuzzy vault scheme, Juels, RSA, 2002	Theory only	×	×	○
Anonymous Biometrics, Linnartz, 2003	Theory and voice	×	×	△
Fingerprint vault, Clancy, 2003	Fingerprint (minutiae)	×	△	○
Fingerprint vault, Uldag, 2003	Fingerprint (minutiae line)	×	△	○
Fingerprint vault, Yang, 2004	Fingerprint (minutiae triple)	○	△	○

Outline

- Background
- Threats of biometrics template leakage
- Methods of template protection
- Implementation of template protection
- Problems to be solved
- Conclusion

Remaining Problem

- Trade-off between safety and robustness.
  - Private Template is backward compatible. But, it is not very safe against attack.
  - Key hiding is safer, but, not as safe as key generation. Robustness is unknown.
  - Key generation is safest, but error recovery of minutiae detection requires a lot of computation to find possible matches and it will result in reduced safety. (more false match)
  - Most of the methods are less robust against alignment error and burst error of minutiae templates.

Conclusion

- Survey of template protection techniques.
  - Private template: transform / scramble
  - Key hiding: encrypted template and hidden secret key
  - Key generation: encrypted template and generation of secret key
  - Key generation is most promising.
  - Application level implementation is not done yet.
- Future direction
  - Solve the trade-off between safety and robustness against positional error and unstable minutiae.

Thank You!