ICPR 2020

Cancelable Biometrics Vault: A Secure Key-Binding Biometric Cryptosystem based on Chaffing and Winnowing

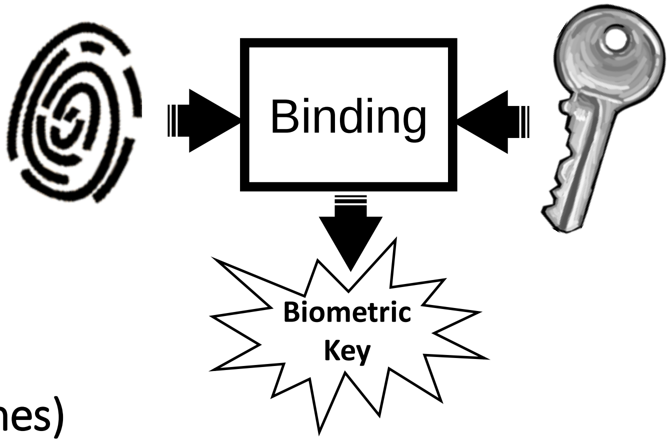
Osama Ouda[a], Karthik Nandakumar[b], Arun Ross[c]

[a]Jouf University, Saudi Arabia

[b]Mohamad Bin Zayed University of Artificial Intelligence, UAE

[c]Michigan State University, USA

Motivation



Key-binding biometric cryptosystems:

- secure cryptographic keys using biometric data.
- protect biometric templates

Existing Techniques (e.g. Fuzzy Commitment and Vault Schemes)

- employ Error Correcting Codes (ECCs) to handle intra-user variations
- trade-off between key length and matching accuracy
- vulnerable to privacy leakage

Novel biometric cryptosystems that deal with these limitations are required

Proposed Method

Cancelable Biometrics Vault (CBV)

A novel biometric cryptosystems based on:

- Cancelable Biometrics (CB)
- Chaffing and Winnowing

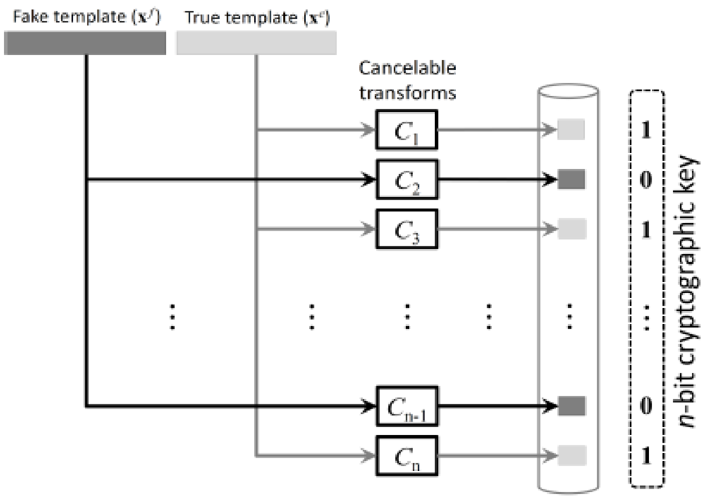
Cancelable Biometrics

- apply different non-invertible transforms to biometric data

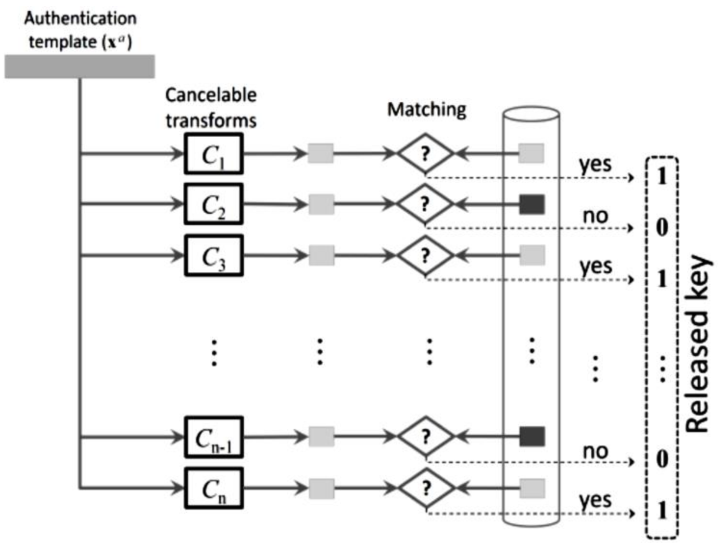
Chaffing and Winnowing

- interleave true data (wheat) with bogus data (chaff)
- to obtain true data, chaff data is winnowed

$$\kappa_{bio}(i) = \begin{cases} C_i(\mathbf{x}^e) & \text{if } \kappa_i = 1; \\ C_i(\mathbf{x}^f) & \text{otherwise} \end{cases}$$



(a) Key-binding procedure.



(b) Key-release procedure.

Proposed Method

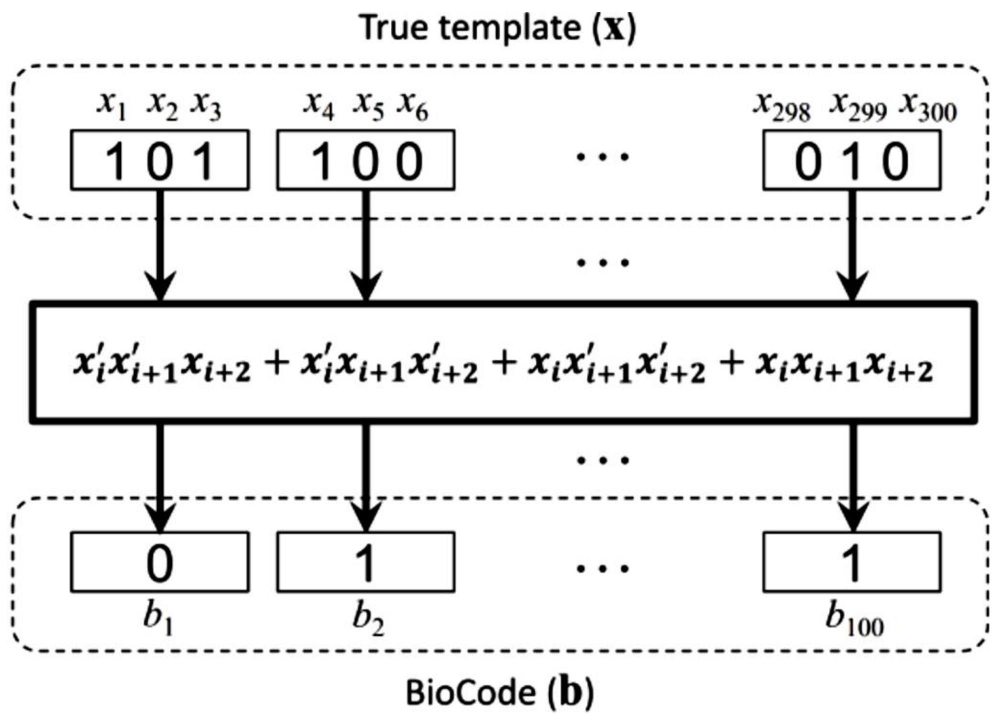
Extended BioEncoding

CB requirements

- Accuracy preservation
- Non-invertibility
- Non-linkability

Extended BioEncoding

To demonstrate the usefulness of the proposed CBV framework



$$f(x_1, x_2, ..., x_m) = x_1 \oplus x_2 \oplus ... \oplus x_m$$
$$f'(x_1, x_2, ..., x_m) = x_1 \odot x_2 \odot ... \odot x_m$$

Results

Recognition Accuracy

- CASIA-V3-Interval iris image database
- 2639 images, 396 classes
- Open-Source Code by Masek

	FRR(%)	FAR(%)
Iris-codes (mask)	4.72	0.001
Iris-codes (generic mask)	5.65	0.001
BioCodes	6.89	0.001
Proposed Method ($\|\kappa\| = 16$)	6.92	0.001
Proposed Method ($\|\kappa\| = 32$)	6.92	0.001
Proposed Method ($\|\kappa\| = 64$)	6.92	0.001
Proposed Method ($\|\kappa\| = 128$)	6.92	0.001
Proposed Method ($\|\kappa\| = 256$)	6.92	0.001

- Decoding accuracy of CBV is comparable to the recognition accuracy of the extended BioEncoding scheme.
- Decoding accuracy is not affected by increasing the key length.

Conclusions

- Novel key-binding biometric cryptosystem framework (CBV) that benefits from CB and chaffing and winnowing.

- Extended BioEncoding CB scheme has been utilized to demonstrate the usefulness CBV.

- Theoretical analysis and experimental results showed that the proposed CBV framework exhibits a number of advantages:

  (i) unlike existing systems, the proposed framework does not employ error correcting codes and thereby it does not impose any restrictions on the key size;

  (ii) there is no trade-off between the key-size and decoding accuracy;

- The proposed framework, however, assumes the availability of suitable CB schemes in order to be applied to different biometric modalities.

- Also, the CBV framework requires the repeated application of the utilized CB scheme (based on the key size) and hence requires powerful processing capabilities.

Thank you very much