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

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

[a]Department of Computer Science, Jouf University, Saudi Arabia
[b]Computer Vision Department, Mohamad Bin Zayed University of Artificial Intelligence, Abu Dhabi, UAE
[c]Department of Computer Science and Engineering, Michigan State University

ABSTRACT

- A novel biometric cryptosystem framework, referred to as Cancelable Biometric Vault (CBV), is proposed.
- The CBV framework benefits from the cancelable biometrics (CB) construct and the concept of chaffing and winnowing to address the limitations of existing biometric cryptosystems.
- To demonstrate the usefulness of the CBV, we implement the framework using the BioEncoding CB scheme.
- Experiments show that the decoding accuracy of the proposed CBV framework is comparable to the recognition accuracy of BioEncoding scheme, regardless of the cryptographic key size.

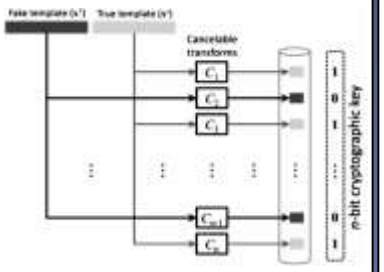
INTRODUCTION

- Biometric cryptosystems are utilized to protect both cryptographic keys and biometrics data.
- Existing techniques such as Fuzzy Commitment and and Fuzzy Vault schemes employ Error Correcting Codes (ECCs) in order to deal with intra-user variations inherent to biometric data.
- This introduces a trade-off between the key length and matching accuracy.
- Moreover, these techniques are vulnerable to privacy leakage since it is it is trivial to recover the original biometric data given the biometric key and its associated cryptographic key.
- In order to address the above two limitations, novel key-binding biometric cryptosystem that does not utilize ECCs is proposed.

PROPOSED CBV FRAMEWORK

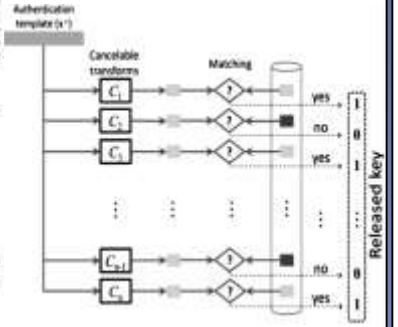
Key Encoding

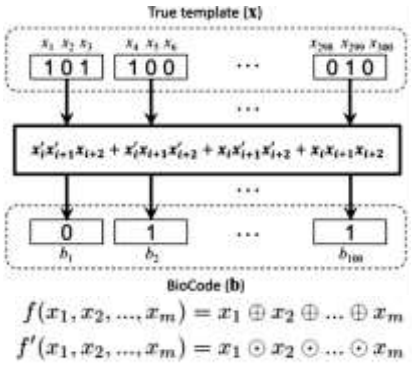
Algorithm 1 Key-binding procedure of the proposed CBV framework.
INPUT: True template $\mathbf{x}^t$, fake template $\mathbf{x}^f$, ℓ-bit random cryptographic key κ, and a set of ℓ cancelable transforms $\{C_i\}_{i=1}^{\ell}$.
OUTPUT: Biometric key κ_{bio}, $Hash(\kappa)$
1: Compute the hash value $Hash(\kappa)$ of the input key κ
2: **for all** bits κ_i in κ **do**
3: **if** $\kappa_i = 1$ **then**
4: $\kappa_{bio}(i) \leftarrow C_i(\mathbf{x}^t)$
5: **else**
6: $\kappa_{bio}(i) \leftarrow C_i(\mathbf{x}^f)$
7: **end if**
8: **end for**



Key Decoding

Algorithm 2 Key-release procedure of the proposed CBV framework.
INPUT: Biometric key κ_{bio}, releasing template $\mathbf{x}^a$, $Hash(\kappa)$, similarity threshold τ, and the same set of ℓ cancelable transforms $\{C_i\}_{i=1}^{\ell}$ used in Algorithm 1.
OUTPUT: Released key κ or Failure
1: Generate ℓ cancelable templates from $\mathbf{x}^a$ using the transforms $\{C_i\}_{i=1}^{\ell}$ employed at key-binding
2: **for all** cancelable templates in κ_{bio} **do**
3: **if** $Sim(\kappa_{bio}(i), C_i(\mathbf{x}^a)) > \tau$ **then**
4: $\kappa'_i \leftarrow 1$
5: **else**
6: $\kappa'_i \leftarrow 0$
7: **end if**
8: **end for**
9: Compute the hash value $Hash(\kappa')$ of the recovered key κ' using the same hashing function employed at binding
10: **if** $Hash(\kappa') = Hash(\kappa)$ **then**
11: Release the key
12: **else**
13: return Failure
14: **end if**



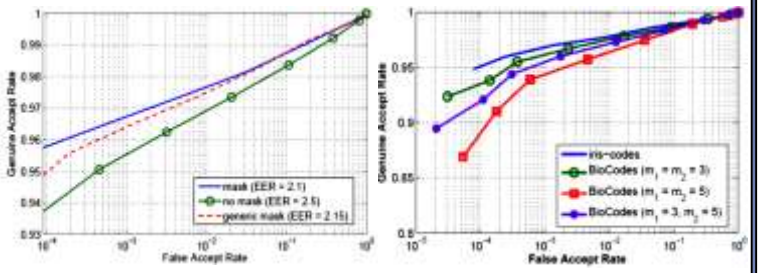


Extended BioEncoding

- An extended BioEncoding CB scheme is used to demonstrate the usefulness of the CBV framework.
- The main idea behind this scheme is to divide the binary template (the iris-code) into words of different lengths and map each word to a single bit based on a non-invertible Boolean function such as the XOR or XNOR functions.

RESULTS

- CASIA-V3-Interval iris image database
- 2639 images, 396 classes
- Open-Source Code by Libor Masek
- A generic mask is used to preserve users' privacy



- 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.

	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

CONCLUSIONS

- Unlike existing systems, the proposed CBV framework does not employ error correcting codes and thereby it deal with the trade-off between the key-size and decoding accuracy.
- Moreover, the CBV does not rely on a specific representation of biometric data.
- The proposed framework, however, assumes the availability of suitable CB schemes so that it can be applied to different biometric modalities.
- Also, the CBV framework requires the repeated application of the utilized CB scheme (proportional to the key size).