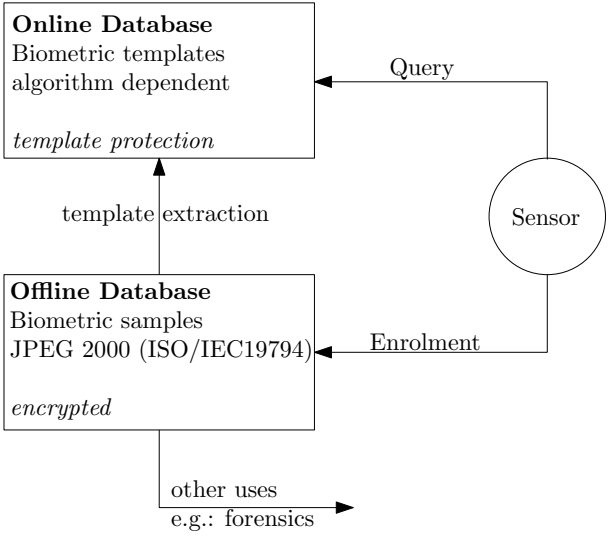
# Highly Efficient Protection of Biometric Face Samples with Selective JPEG2000 Encryption

*Hofbauer*[1], Martínez-Díaz[2], Kirchgasser[1], Méndez-Vázquez[2], Uhl[1]
[1]University of Salzburg
[2]Advanced Technologies Application Center, Havana

ICASSP'21
Paper #1610

This project received funding from EU Horizon 2020 research program under grant agreement No. 690907 and from the Austrian Science Fund under project No. P27776.

# Introduction I



# Introduction II

We investigate a lightweight JPEG2000 encryption scheme for compressed face data.

- selective bit-stream protection using AES
- no reduced recognition accuracy
- low computational effort

Drawback: a certain amount of data is left in plain text

- security analysis is required (similar to template protection)
- impact of JPEG2000 coding
  - layer progression
  - resolution progression
  - encryption amount and position for optimal protection/speed

# Evaluation Methodology I

JPEG 2000 based parameters:

- Evaluate layer and resolution progression (JPEG 2000)

Biometric based parameters:

- Where is the most relevant information for the face recognition algorithms?
- What is the minimum amount of encryption required to protect the biometric face sample?

Focus is on the beginning of the codestream:

- Beginning: Structural data
- Towards end: refinement for fine textures.
- face information depends on structural data

# Evaluation Methodology II

***Sliding Window Encryption*** to detect the location of relevant data.

- A small part of the codestream is encrypted (window)
- Offset is varied (sliding window)

***Increasing Window Encryption*** to find the minimum encryption emount.

- Offset is fixed from the beginning (no sliding window).
- Encryption amount is increased.

# Evaluation Methodology III

Actuall setups:

- **small encryption window** is a sliding window encryption
  - window size is $0.5\%$ of the bitstream
  - offset varies from $0\%$ to $15\%$ in steps of $1\%$
- **large encryption window** is a sliding window encryption
  - window size is $4\%$
  - offset is varied from $0\%$ to $20\%$ in $2\%$ steps
- **increasing encryption window** is an increasing window encryption
  - window size increases from $1\%$ to $15\%$ in steps of $1\%$.

Coding parameters for each of the above tests (progression type):

- **layer progression**
- **resolution progression**

# Evaluation Methodology IV

Face Recognition Methods

- Traditional
  - Local Binary Patterns (LBP)
  - Multi-Block LBP (MBLBP)

Histogram per 14x14 cell region, chi-squared similiarity measure.

- CNN based methods
  - ResNet-ArcFace (ArcFace)
  - MobileFaceNet (MobileFace)
  - ShuffleFaceNet (ShuffleFace)

# Dataset I

- The Labeled Faces in the Wild (LFW) database
  - $13,233$ face images
  - $5,749$ different identities
  - large variations in pose, expression and illumination
- 10-fold split of $6000$ face pairs each
- face images were aligned and cropped
  - 112x112 pixel
  - RetinaFace detector
  - JPEG2000 encryption on cropped image

# Dataset II

An illustration: **Small encryption window**
Offset as given in both layer and resolution progression.

Original

layer progression

00 01 02 03 04 05 06 07

08 09 10 11 12 13 14 15

resolution progression

00 01 02 03 04 05 06 07

08 09 10 11 12 13 14 15

# Dataset III

An illustration how this looks in practice.
Layer progression

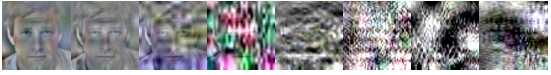
Original

**large window encryption**

00 01 02 03 04 05 06 07

08 09 10 11 12 13 14 15

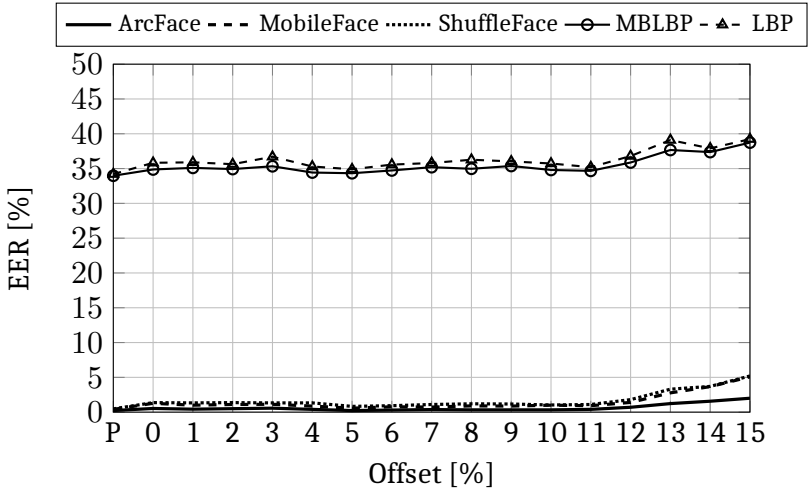
**increasing window encryption**



01 02 03 04 05 06 07 08

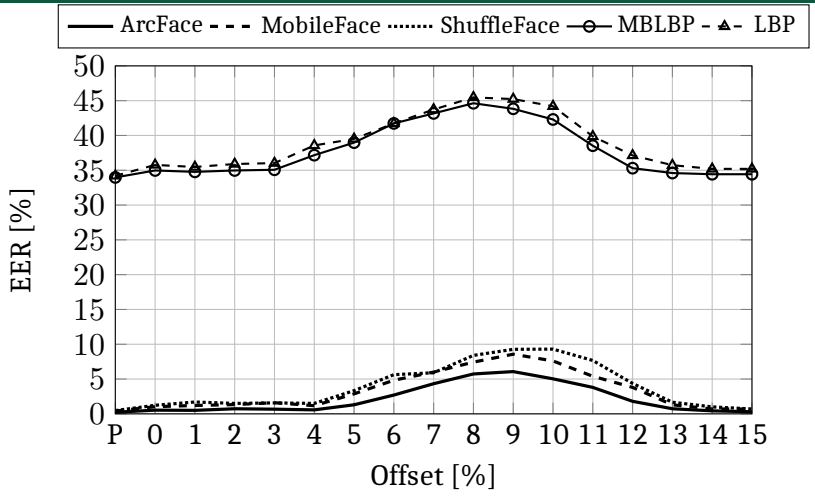
09 10 11 12 13 14 15 16

# Evaluation—Small Window Encryption I



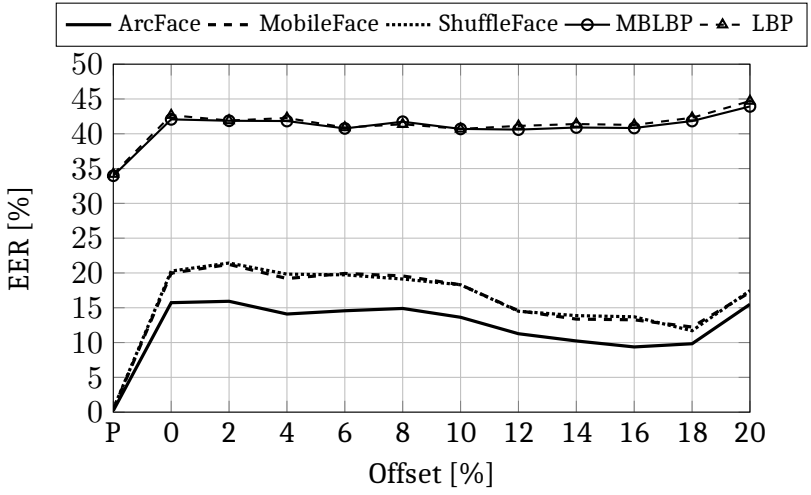

*Resolution progression with error correction.*

# Evaluation—Small Window Encryption II



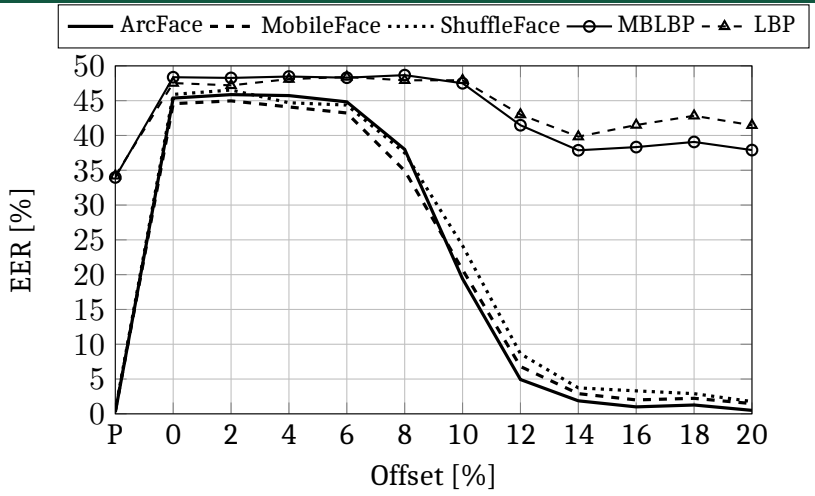

*Layer progression with error correction.*

# Evaluation—Large Window Encryption I



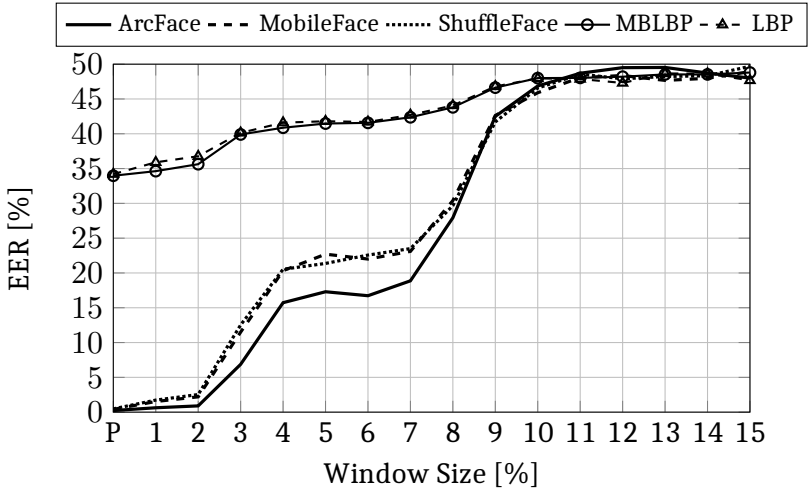

*Resolution progression with error correction.*

# Evaluation—Large Window Encryption II



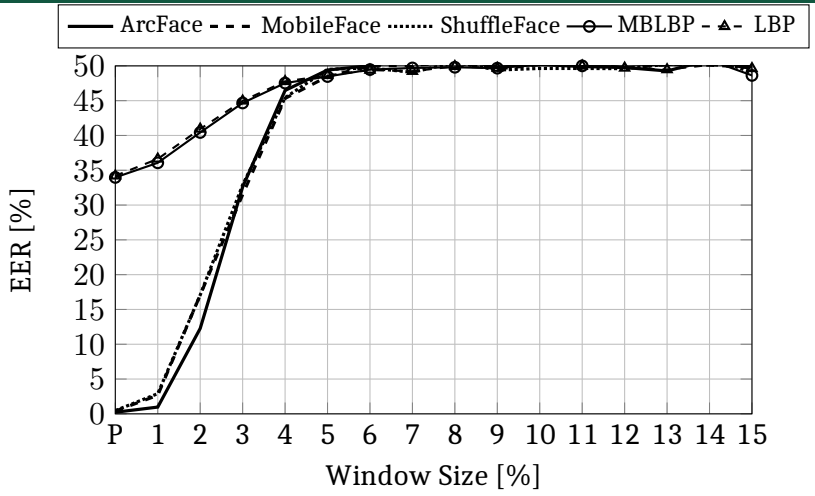

*Layer progression with error correction.*

# Evaluation—Increasing Window Encryption I




*Resolution progression with error correction.*

# Evaluation—Increasing Window Encryption II




*Layer progression with error correction.*

# Conclusion

- Traditional and deep learning based methods exhibit an identical behavior.
- Faster traditional methods can be used for analysis of selective encryption options.
- When **storing** facial biometric samples with JPEG2000 it is recommended to use the **layer progression type**.
- The **relevant** part for biometric face recognition is at around **4–12%** of the total codestream.
- The most **secure** method for encryption is to start at the **beginning and at least include the first 12%**.