Highly Efficient Protection of Biometric Face Samples with Selective JPEG2000 Encryption

Heinz Hofbauer[†] ● Yoanna Martínez-Díaz[‡] ● Simon Kirchgasser[†] ● Heydi Méndez-Vázquez[‡] ● Andreas Uhl[†]

[†] Paris Lodron University Salzburg (PLUS), Department of Computer Sciences, Salzburg, Austria

[‡] Advanced Technologies Application Center (CENATAV), Havana, CUBA

Paper #1610

Abstract

When biometric databases grow larger, a security breach or leak can affect millions. In order to protect against such a threat, the use of encryption is a natural choice. However, a biometric identification attempt then requires the decryption of a potential huge database, making a traditional approach potentially unfeasible. The use of selective JPEG2000 encryption can reduce the encryption's computational load and enable a secure storage of biometric sample data. In this paper we will show that selective encryption of face biometric samples is secure. We analyze various encoding settings of JPEG2000, selective encryption parameters on the "Labeled Faces in the Wild" database and apply several traditional and deep learning based face recognition methods.

Main Results

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

Introduction

International Organisation for Standardisation (ISO)

- biometric data to be recorded and stored as JPEG or JPEG2000
- Several studies recommending JPEG2000 over JPEG

Online-database (biometric templates)

- protected by template protection schemes

Offline-database (biometric samples)

- protected by state of the art cypher (AES)
- access required decryption
- time consuming if whole database is required
  - change of biometric comparison or template extraction
  - regeneration of the template protection key (to guard against attacks)

Lightweight JPEG2000 encryption scheme for compressed face data

+ selective bit-stream protection using AES: secure, no loss of recognition accuracy

+ low computational effort

– *some data left in plaintext → requires security analysis*

Selective JPEG2000 security analysis

JPEG2000 coding settings

- resolution progression
- layer progression

Question one: Where is the most relevant information for the face recognition algorithms

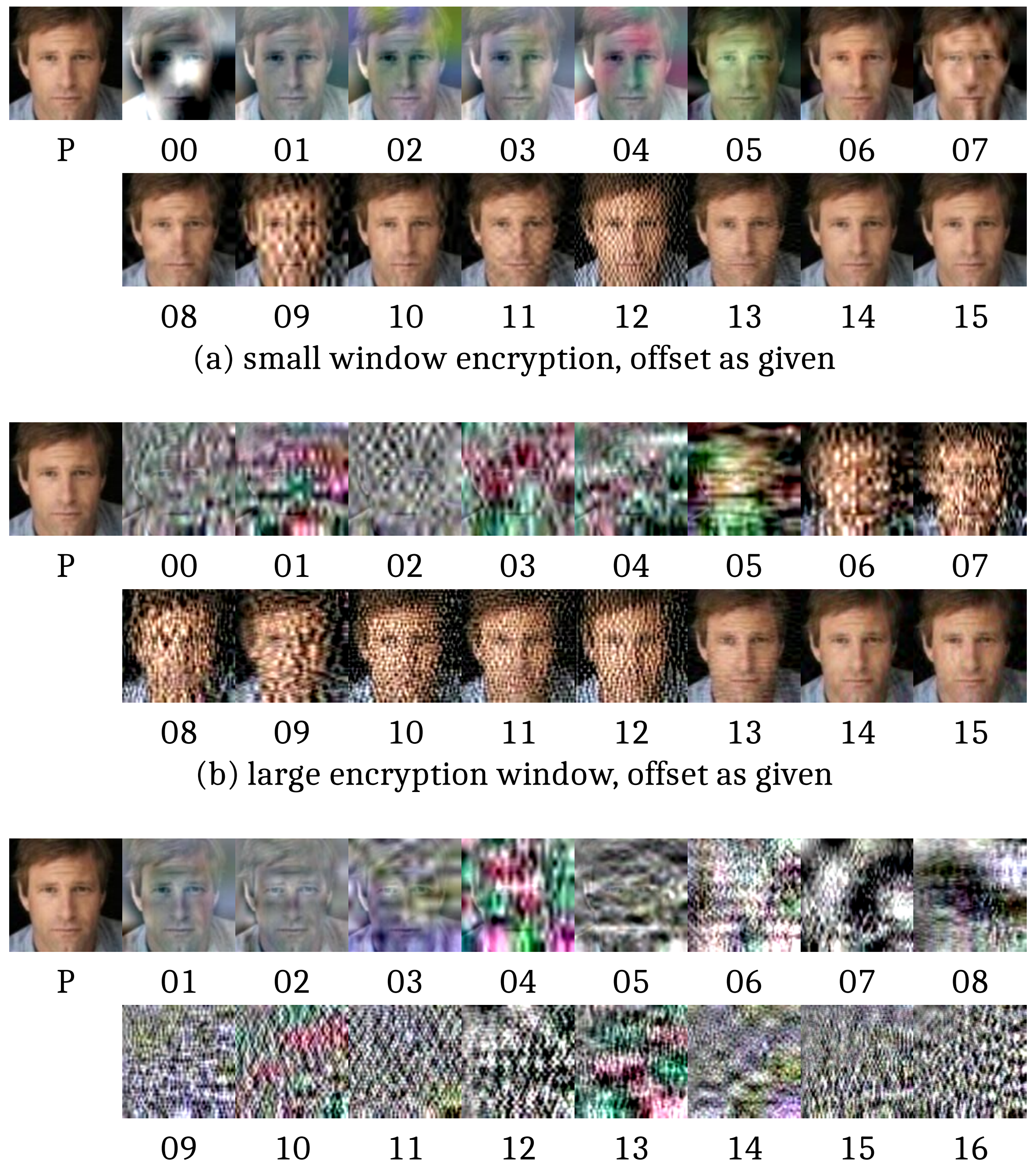
- A fixed percentage of the codestream is encrypted, position is varied.
- *small encryption window*—The size of the sliding window is fixed to 0.5% of the bitstream, the offset varies from 0% to 15% in steps of 1%
- *large encryption window*—The sliding window is increased, but still fixed, in size to 4%, the offset is varied from 0% to 20% in 2% steps

Question two: What is the minimum amount of encryption required to protect the biometric face sample

- *increasing encryption window*—Encryption starts at the beginning (0%) and the encryption amount increases from 1% to 15% in steps of 1%.

Face Recognition Methods

- Traditional methods, compared with χ^2 similarity measure:
  - Local Binary Patterns (LBP)
  - Multi-Block LBP (MBLBP)
- Deep convolutional neural networks, compared with cosine distance:
  - ResNet-ArcFace (ArcFace)
  - MobileFaceNet (MobileFace)
  - ShuffleFaceNet (ShuffleFace)



(a) small window encryption, offset as given

(b) large encryption window, offset as given

(c) increasing encryption window, encryption amount as given

Figure 1: Sample from the faces in the wild database, Aaron Eckhart #1, with layer progression. The original is also shown labled P.

Data for Experiments

Labeled Faces in the Wild (LFW) database

- well known public database
- 13, 233 face images
- 5, 749 different identities
- large variations in pose, expression and illumination

An example with the different encryption types is given in 1.

Evaluation and Training

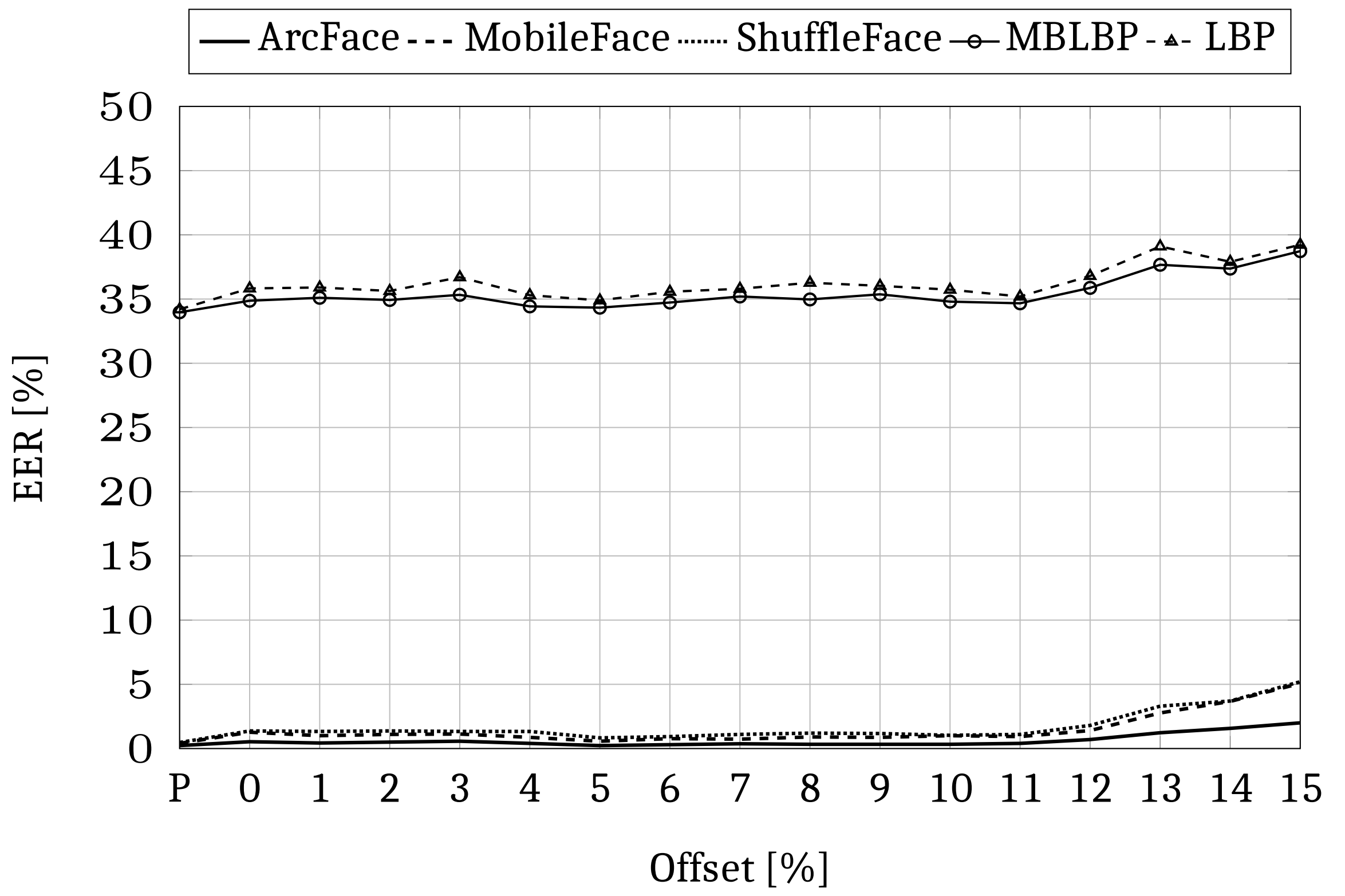
- 10-fold split of 6000 face pairs
- images were aligned and cropped (to 112×112 pixel) by using the RetinaFace detector

The equal error rate (EER)

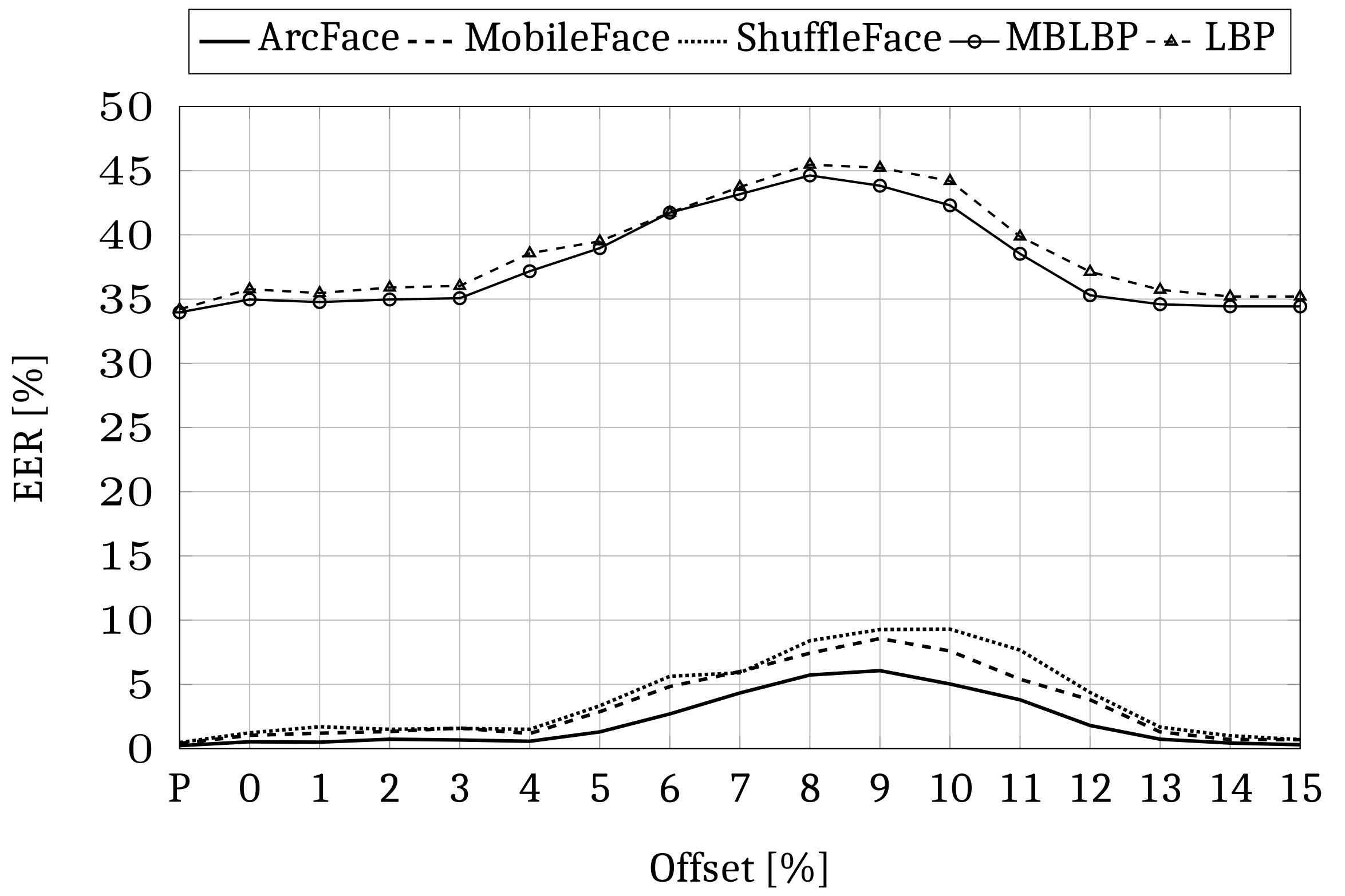
- Mean accuracy and area under curve agree with the EER and aren't given
- 50% EER is guessing (protected samples can't be used for comparison)

Evaluation—small window encryption

Equal error rates for the small encryption window with offset moving from 0 to 15% and the unencrypted baseline (**P**).



Resolution progression with error correction.

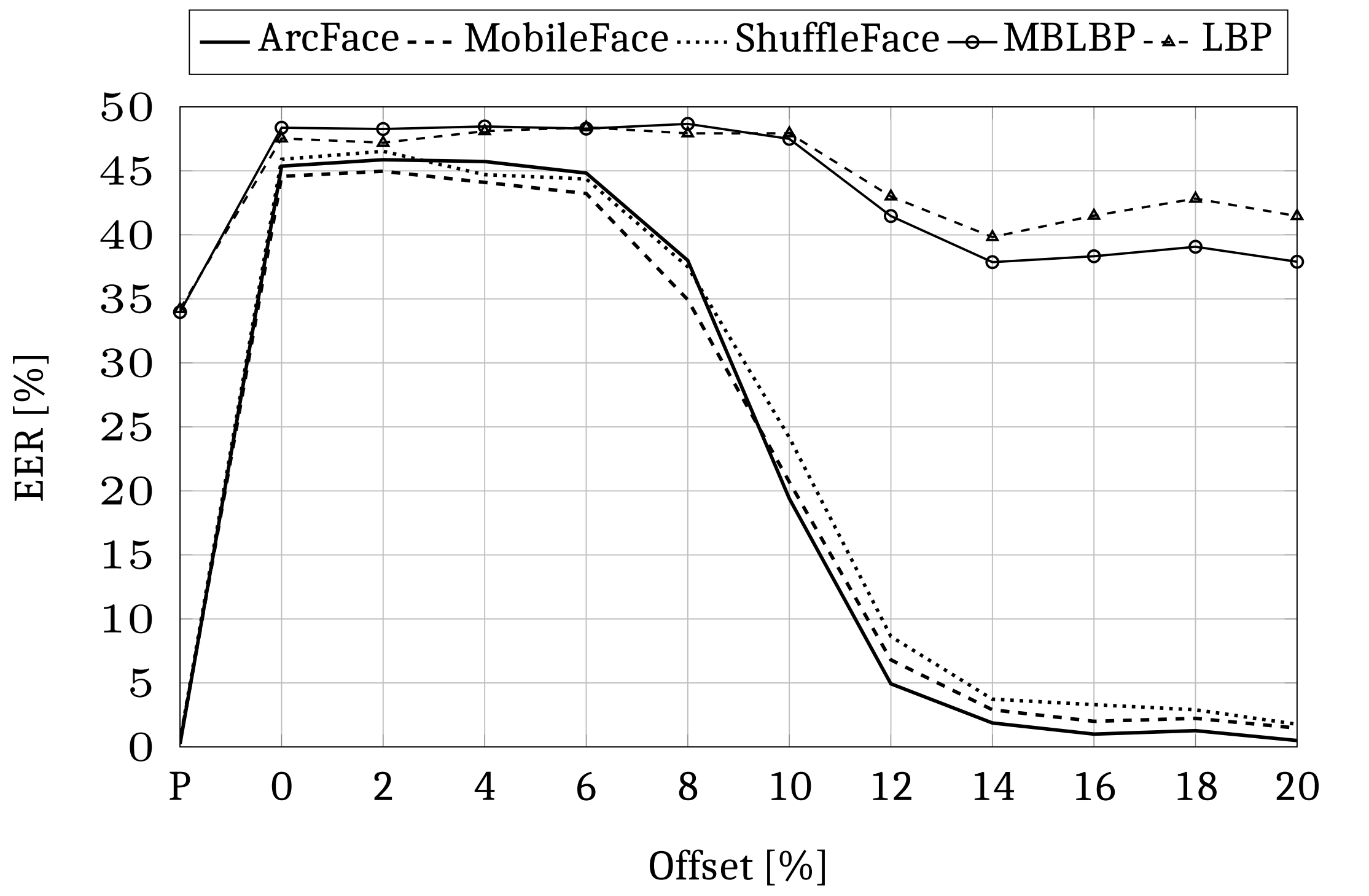


Layer progression with error correction.

- The encryption window size of 0.5% has a negligible impact on the recognition performance and can not be considered secure.
- Deep learning methods outperform traditional methods.
- Traditional methods (LBP and MBLBP) act similarly to the deep learning based methods.
- Training and evaluation of deep learning methods takes longer.
- Important structure for biometric recognition is localized in layer progression mode between 4% – 14%.
- Layer is in all following cases the better methods because it condenses the important structure. Progression will no longer be shown.

Large Encryption Window Evaluation

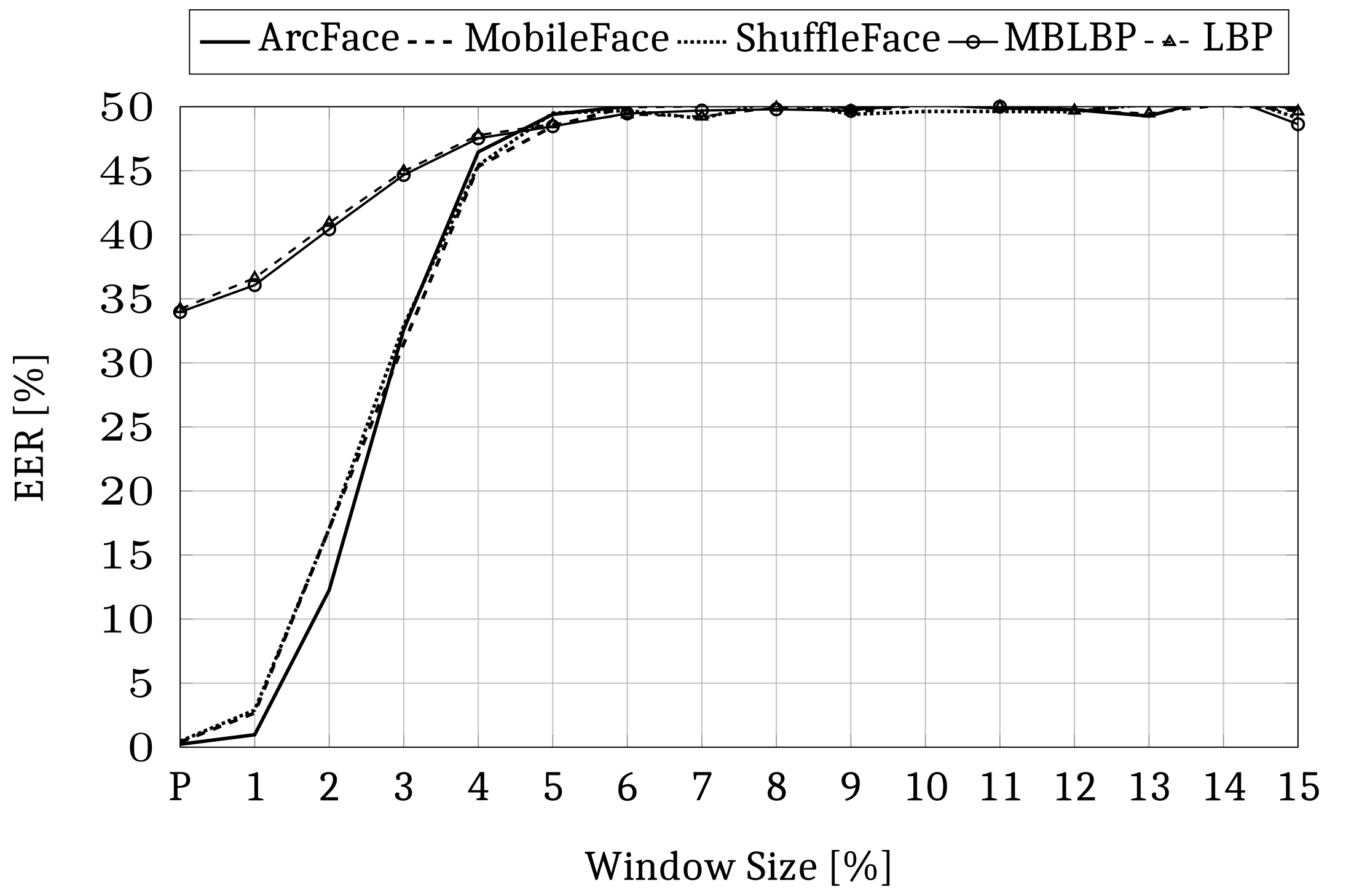
Equal error rates for the large encryption window with offset from 0 to 20% and the unencrypted baseline (**P**). Only layer progression is shown.



- For layer progression almost sufficient to protect the sample (≈ 50%)
- Encryption of the structural information, from 0% – 4%, also is sufficient for the protection of the biometric sample
- The removal of the basic structure makes the refinement information (4% – 14% see small window encryption) unusable

Increasing Encryption Window Size

Equal error rates for the increasing window encryption with a size of 1 to 15% and the unencrypted baseline (**P**). Layer progression only.



- For layer progression security is reached when encrypting the coarse structure that lies between 5% and 12%.
- For resolution progression (not shown) requires more encryption for security. This is slower and not recommended.