Privacy-Preserving Face Recognition Using Noised Eigenvectors

1st Bruce L'Horset
Software Engineering
Paris Institute of Digital Technology
Paris, France
bruce.lhorset@eleve.isep.fr

2nd Charles Mailley
Software Engineering
Paris Institute of Digital Technology
Paris, France
charles.mailley@eleve.isep.fr

3rd Elodie Chen
Software Engineering
Paris Institute of Digital Technology
Paris, France
elodie.chen@eleve.isep.fr

4th Sara Ricci
Department of Telecommunication
Brno University of Technology
Brno, Czech Republic
0000-0003-0842-4951

***Abstract*—Widespread face recognition systems raise significant privacy concerns due to potential data exposure, especially with centralized data storage.**

We propose a privacy-preserving framework integrating k-same pixelation, Principal Component Analysis (PCA), and Differential Privacy (DP).

Our pipeline applies k-same smoothing for initial feature averaging, uses PCA for dimensionality reduction while preserving essential facial features, and adds Laplace noise to the resulting projection vectors to achieve DP. This method masks biometric information, operating efficiently in the lower-dimensional PCA space, aiming to balance privacy protection with the utility needed for identity verification.

Evaluations on the LFW dataset quantitatively analyze this trade-off using MSE and SSIM metrics. Results confirm integrating DP enhances privacy. Crucially, experiments show adding noise to lower-dimensional projection vectors preserves utility better than noising higher-dimensional eigenfaces.

We identified parameters (k=10, PCA ratio=0.19, ϵn=0.24) yielding a practical balance (Avg. MSE 1499, Avg. SSIM 0.38), enabling effective machine recognition on the anonymized data and demonstrating the framework's viability.

***Index Terms*—K-Same Pixel, Eigenface, Laplace Noise Addition, Differential Privacy, Facial Recognition, Biometric Authentication.**

I. Introduction

Face recognition (FR) [5] is ubiquitous in modern security, authentication, and surveillance systems. However, this reliance raises significant privacy concerns due to potential misuse or exposure of sensitive biometric data, leading to risks like identity theft, especially when centralized. Addressing these risks requires robust privacy-preserving techniques to effectively balance security and system utility. While traditional encryption protects stored data, it is often too computationally intensive for demanding real-time FR applications.

Alternatives like Differential Privacy (DP) [1] and k-anonymity [4] offer promising directions. These methods introduce controlled noise or anonymization, aiming to protect individual identities while still permitting necessary aggregate analysis or verification tasks. This paper develops and evaluates a specific framework integrating such techniques for practical, privacy-enhanced face recognition deployment.

A. Contribution

In this work, we propose a privacy-preserving framework applying: (1) K-Same pixelation for smoothing facial characteristics, (2) Principal Component Analysis (PCA) [3] for dimensionality reduction and feature extraction, and (3) controlled Laplacian noise for anonymization, aiming to balance privacy and recognition utility. Our scheme enhances [1] by incorporating K-Same pixelation and experimental results favouring eigenvectors over eigenfaces.

We developed a user-friendly Graphical User Interface (GUI) to apply different anonymization levels and visualize the privacy-utility trade-off. Evaluation using Mean Squared Error (MSE) and Structural Similarity Index Measure (SSIM) metrics helps identify optimal approaches for secure face recognition.

II. Architecture and Analysis Method

The system has been built using the Flask package in Python, enabling deployment as either a website server or a desktop application. Flask provides a straightforward and standardized way to create websites in Python, clearly separating the front-end components from the back-end logic.

The primary goal of this application is to serve as an experimental tool, allowing users to adjust various parameters to generate noised images, attempt to reconstruct the resulting images and verify the existence of a user in the database. The secondary goal is to provide users with optimal parameters for each step of the noised image generation process. To accomplish this, the application includes analyses and graphs that justify the choice of specific parameter values.

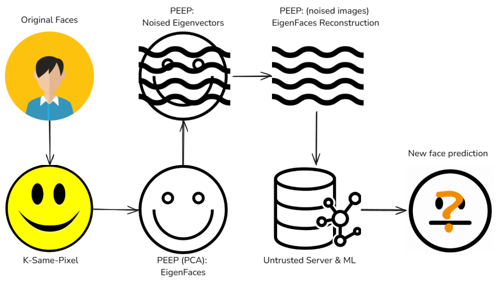


Fig. 1. Anonymization Process Schematic

The image anonymization process follows the steps illustrated in Fig. 1. Starting with a list of front-facing photos, the anonymization mechanism applies 1) K-same pixel method, 2) PCA and, finally 3) differential privacy and, finally 4) create noised images. This produces a list of anonymized images that can be stored in an untrusted database. On the other hand, to evaluate the privacy-utility trade-off, the final step involves reconstructing the user's face and comparing the reconstructed image with the original photo provided.

The PCA algorithm generate both eigenfaces and eigenvectors. Noised images are reconstructed from noised eigenvectors using the existing PCA model, while eigenfaces are used solely for visual verification purposes.

III. Back-end and Front-end Architecture

The Controller object orchestrates the various steps of image processing. This approach enables an autonomous workflow for the GUI application while also allowing the creation of multiple analysis objects. These objects can be used to develop and test functions independently.

The back-end application starts by taking a data set as input. PCA is used to extract eigenfaces and eigenvectors from the input images. DP mechanism is then applied on eigenvectors. Using the precomputed PCA model and the noised eigenvectors, noised images are then reconstructed, enhancing security and privacy.

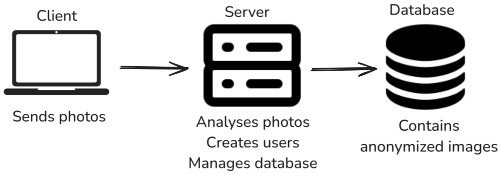
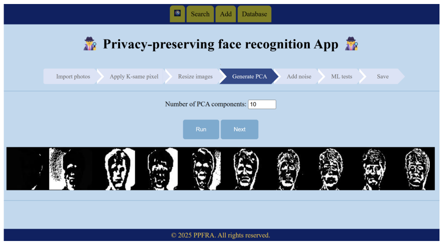


Fig. 2. Front-End Architecture

For the front-end, the application runs locally, meaning the client, server, and database are all managed on the user's laptop. However, in a web-based implementation, the database would reside on untrusted third-party servers, as illustrated in Fig. 2. The database used is a simple SQLite file containing a single table with two columns: the user ID and the anonymized images.



Number of PCA components: 10

Fig. 3. Screenshot of the application

Fig. 3 shows the front-end application layout. The application comprises three main functional components: adding new users to the database, verifying if a user exists within the database, and managing the database's contents. The new user page enables the creation of new users using the PEEP method, requiring a set of front-facing photos of the same individual. The database management page allows users to display, remove, or attempt reconstruction of stored images.

IV. Experimental Results

This section details the experimental setup, parameter selection, and analysis of the trade-off between privacy and utility conducted on the Labeled Faces in the Wild (LFW) dataset. LFW was chosen for its representation of faces in less constrained, real-world conditions, providing a robust testbed for our privacy preserving pipeline.

A. Metrics Definition

To evaluate the quality of image reconstruction and the impact of anonymization, we use two primary metrics: Mean Squared Error (MSE) and Structural Similarity Index Measure (SSIM).

Mean Squared Error (MSE): The MSE quantifies the pixel-wise difference between the original and reconstructed images. It is calculated as the average of the squared intensity differences for all pixels. A lower MSE value indicates a higher fidelity reconstruction, meaning the reconstructed image is closer to the original. High MSE values suggest significant distortion.

Structural Similarity Index Measure (SSIM): The SSIM assesses the perceived similarity between two images by considering luminance, contrast, and structure. SSIM values range from -1 to 1, where 1 signifies perfect similarity. Values closer to 1 indicate that the structural information, crucial for visual perception and potentially recognition, is well preserved.

In our privacy-preserving context, these metrics serve a dual purpose. Before noise addition, low MSE and high SSIM validate the PCA reconstruction quality. After noise addition for differential privacy, we aim for a controlled increase in MSE and decrease in SSIM. The goal is to find a balance where MSE is high enough to hinder human visual recognition, while SSIM remains sufficient for machine-based recognition systems. This balance is explored through parameter tuning.

B. Experimental Setup Overview

Our pipeline applied to the LFW dataset involved several steps. We used a subset of LFW containing individuals with at least 20 images each, ensuring sufficient data per subject for subsequent analysis. The core steps included K-Same pixelation, PCA dimensionality reduction, and Differential Privacy noise addition. The selection of parameters for each step was guided by analyzing their impact both quantitatively (metrics trends) and qualitatively (visual results), as detailed in the following subsections.

C. K-Same Pixelation Analysis

The K-Same pixel technique averages pixel values across ‘k‘ images of the same subject, providing initial smoothing and anonymization. We analyzed the effect of varying ‘k‘ on reconstruction metrics (MSE/SSIM after this step, before PCA/noise). The trend graph 4 shows how distortion (MSE) increases and similarity (SSIM) decreases as ‘k‘ increases. Based purely on finding an intersection point between hypothetical MSE/SSIM thresholds on this trend graph, a value like k=9 might appear optimal. Visual inspection of the resulting images for different ‘k‘ values on Fig. 5 further illustrates the trade-off between the smoothing effect and the preservation of distinct facial features.

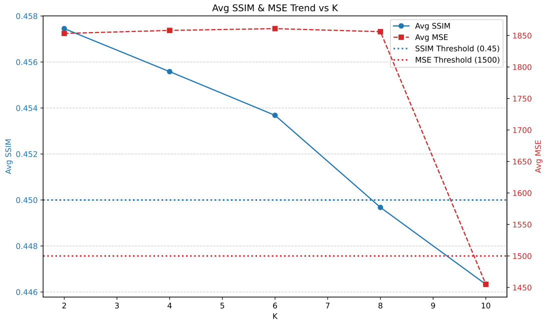


Fig. 4. MSE/SSIM of k-value trend graph

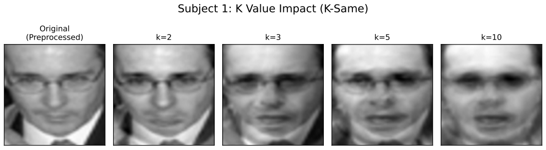


Fig. 5. K-Same Visual Impact

D. PCA Dimensionality Reduction Analysis

Principal Component Analysis (PCA) reduces data dimensionality. We evaluated the reconstruction quality (MSE/SSIM, measured *before* noise addition) versus the number of principal components retained (expressed as a ratio of available components). The trend graph 6 shows reconstruction fidelity improving with higher ratios. Visual analysis of the graph suggests that an approximate optimal ratio could be around 0.55. However, visual examples on Fig. 6 demonstrate that perceptual gains can become marginal beyond a certain point, while computational load increases. This analysis helps identify ratios that capture essential features without unnecessary overhead.

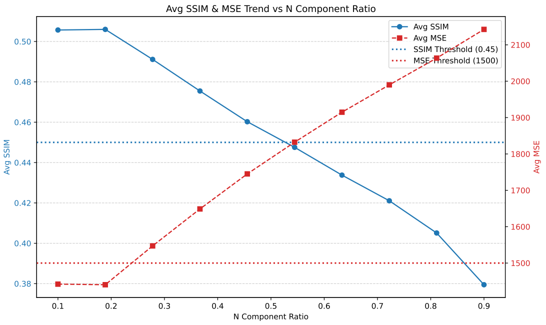


Fig. 6. MSE/SSIM of PCA Component ratio trend graph

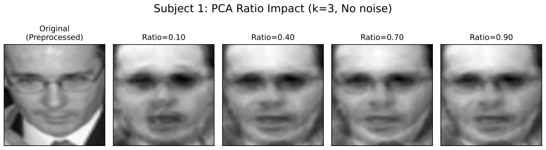


Fig. 7. PCA Component ratio Visual Impact

E. Differential Privacy Noise Analysis

Laplace noise was added to the projection vectors (coefficients obtained from PCA) to ensure ϵ-differential privacy. Adding noise to these lower-dimensional vectors is preferred over adding noise directly to eigenfaces for better utility preservation. The privacy parameter epsilon (ϵ) controls the noise level: lower ϵ means more noise and stronger privacy guarantees. Trend graph 8 shows MSE increasing and SSIM decreasing as ϵ gets smaller (more noise). Observation of the graph indicates that a value of approximately 0.2 for ϵ appears relevant, as the MSE and SSIM curves intersect while remaining within their respective acceptable thresholds. Visual examples on Fig. 9 illustrate the increasing image distortion with lower ϵ values.

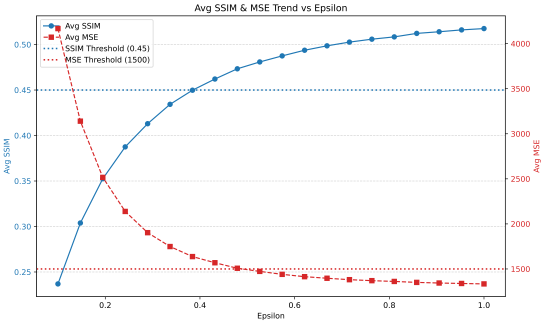


Fig. 8. MSE/SSIM of k-value trend graph

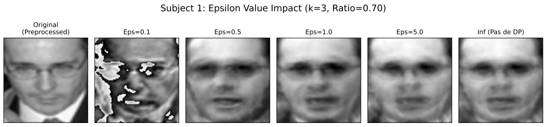


Fig. 9. K-Same Visual Impact

F. Selected Parameter Combination

While individual analyses (Sections IV.C, IV.D, IV.E) might suggest specific optimal points for each parameter (like k=9 from Fig. 4), the final parameter selection must consider their combined effects on both privacy and utility. A multi-objective perspective, potentially visualized through a density and scatter plot showing performance across combinations on Fig. 10, is necessary. This visualization helps identify Pareto optimal points or regions that satisfy specific constraints (e.g., minimum acceptable utility, maximum tolerable distortion).

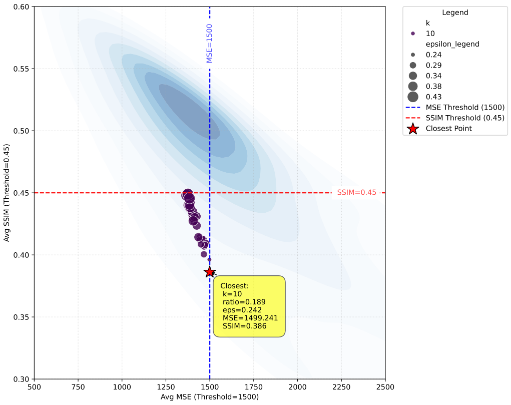


Fig. 10. Privacy-utility performance density graph for various (k, ratio, ϵ)

Based on such an analysis, aiming for robust machine recognition while ensuring significant visual distortion, the combination k=10, PCA ratio=0.19, and ϵ=0.24 (marked with a star in Fig. 10) was selected for the main experiments reported in this paper. This specific parameter set resulted in an average MSE of 1499 and an average SSIM of 0.38 across the processed LFW subset.

G. Machine Recognition Utility

A crucial aspect is evaluating whether the anonymized images, despite the introduced distortions resulting from the chosen parameters (k=10, ratio=0.19, ϵ=0.24), remain useful for automated tasks like face recognition. We trained a simple Convolutional Neural Network (CNN) model exclusively on the anonymized LFW images produced by our pipeline. The training process of the CNN model is illustrated in Fig. 11, showing the convergence of accuracy and loss over epochs, indicating successful learning on the anonymized data.

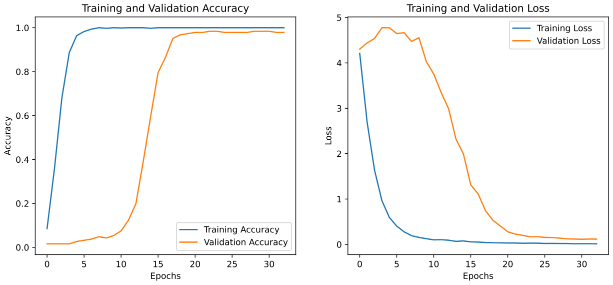


Fig. 11. Accuracy and Loss on anonymized LFW ML training

The model's performance was assessed on a held-out test set of similarly anonymized LFW images. It achieved a classification accuracy of 98%.

H. Privacy-Utility Discussion

The results using k=10, PCA ratio=0.19, and ϵ=0.24 on LFW represent an operating point selected via multi-parameter analysis (Fig. 10). Measured MSE (1499) and SSIM (0.38) quantify privacy (distortion), while ML accuracy (98%) quantifies utility. This demonstrates feasibility on datasets like LFW, retaining utility for automated systems. Achieving a different balance (e.g., stronger privacy or maximum utility) necessitates further exploration guided by trade-off visualizations (Fig. 8, Fig. 10), as the optimal choice depends on application needs.

V. Conclusion

Our framework, using K-Same pixelation, PCA, and Differential Privacy on projection vectors, anonymizes LFW dataset faces while maintaining ML recognition utility. Achieving a suitable balance required careful parameter selection (k=10, ratio=0.19, ϵ=0.24), guided by multi-objective analysis of the privacy-utility trade-off. Applying noise to vectors proved advantageous, and results underscore the need for dataset-specific tuning.

Future Work: Further research could investigate alternative anonymization methods (pixelation, transforms, noise types, adaptive approaches) to explore different privacy-utility profiles. Optimizing ML models using robust architectures for enhanced recognition on anonymized data is another direction. Finally, developing automated techniques for selecting optimal parameters based on specific requirements would improve practical application.

References

[1] Chamikara MA, Bertok P, Khalil I, Liu D, Camtepe S. Privacy preserving face recognition utilizing differential privacy. Computers & Security. 2020 Oct 1;97:101951.

[2] Dosselmann R, Yang XD. A comprehensive assessment of the structural similarity index. Signal, Image and Video Processing. 2011 Mar;5:81-91.

[3] Kim KI, Jung K, Kim HJ. Face recognition using kernel principal component analysis. IEEE signal processing letters. 2002 Feb;9(2):40-2.

[4] Meden B, Emersic Z, Struc V, Peer P. k-Same-Net: k-Anonymity with generative deep neural networks for face deidentification. Entropy. 2018 Jan 13;20(1):60.

[5] Taskiran M, Kahraman N, Erdem CE. Face recognition: Past, present and future (a review). Digital Signal Processing. 2020 Nov 1;106:102809.