Deep Learning Applications for Biometrics Security

Dmytro Zakharov
Supervisor: Oleksandr Kuznetsov

Unrecognizable Yet Identifiable: Image Distortion with Preserved Embeddings

Most state-of-the-art biometrics recognition techniques rely on the concept of *embedding model*.

Definition 1. ***Embedding model*** *is an image-to-vector function* $\mathcal{F} : \mathcal{I} \to \mathbb{R}^m$*, which maps an image to a low-dimensional representation in* $\mathbb{R}^m$ *(typically for* $m \lesssim 1024$*) called* ***embedding****, which preserves small (usually Euclidean) distances between images in the same class and large between images from different classes.*

This way, two face images X and Y can be compared by comparing $\|\mathcal{F}(X) - \mathcal{F}(Y)\|_2$ with a threshold $\tau \in \mathbb{R}_{\geq 0}$. The question arises: based on the image X, is it possible to generate an unrecognizable face image X' such that $\mathcal{F}(X)$ and $\mathcal{F}(X')$ are relatively "close"? Our studies [5, 6] build the *U-Net* deep generator $\mathcal{G} : \mathcal{I} \to \mathcal{I}$ which maps an image to the unrecognizable image, in the traditional sense, which neural network can still identify by comparing photos' embeddings. This generator allows us to build a much more secure biometrics storage: instead of storing $X \in \mathcal{I}$ directly in the database, we store $\mathcal{G}(X)$. We also show that this method is *faster* than widely used cancelable biometrics or image encryption techniques.

Face anti-spoofing model

Based on the image from the scanner, detect whether the image is fake (for example, the attacker shows a photo of another person from the mobile device). In our works, we explore how to build an efficient model that requires minimal resources while still achieving high accuracy. In [4], we use five different datasets and explore how well training on one dataset generalizes to results on four other datasets. In [3], we explore the neural network in more detail and show its supremacy in terms of performance compared to other models. We achieved low error rates for all five datasets presented.

Cryptographic key generation from face images

This research aims to generate a cryptographic key based on the face image. We employ the idea of *fuzzy extractors*: based on two fixed-size binary strings $s_1, s_2 \in \{0, 1\}^\ell$ which are "relatively" close (empirically, the Hamming distance $d_H(s_1, s_2)$ of which is less than roughly $\frac{\ell}{4}$), the *fuzzy extractor* $\phi(\cdot, h)$ maps them to the same output $R \in \{0, 1\}^L$ using public helper string h.

This way, our research papers [2, 1] was primarily dedicated to building the image-to-binary-string function $\psi : \mathcal{I} \to \{0, 1\}^\ell$ which, based on the image of two similar people, output close fixed-size binary strings. Applying ϕ and ψ sequentially would, in turn, generate the desired key. To build ψ, we employ the state-of-the-art *Face Recognition* embedding model with an accuracy of 98%+ on widely used *LFW* and *CelebA* datasets. As a result, we achieve an algorithm with an error rate of less than 10%.

References

[1] Alexandr Kuznetsov et al. "Deep Learning Based Fuzzy Extractor for Generating Strong Keys from Biometric Face Images". In: *2022 IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)*. 2022, pp. 421–426. DOI: 10.1109/PICST57299.2022.10238643.

[2] Oleksandr Kuznetsov, Dmytro Zakharov, and Emanuele Frontoni. "Deep learning-based biometric cryptographic key generation with post-quantum security". In: *Multimedia Tools and Applications* (2023). DOI: 10.1007/s11042-023-17714-7. URL: https://doi.org/10.1007/s11042-023-17714-7.

[3] Oleksandr Kuznetsov et al. *AttackNet: Enhancing Biometric Security via Tailored Convolutional Neural Network Architectures for Liveness Detection*. 2024. arXiv: 2402.03769 [cs.CV].

[4] Oleksandr Kuznetsov et al. "Cross-Database Liveness Detection: Insights from Comparative Biometric Analysis". In: *Proceedings of the 2nd International Workshop on Social Communication and Information Activity in Digital Humanities (SCIA 2023), Lviv, Ukraine, November 9, 2023*. Vol. 3608. CEUR Workshop Proceedings. CEUR-WS.org, 2023, pp. 250–263. URL: https://ceur-ws.org/Vol-3608/paper19.pdf.

[5] Dmytro Zakharov, Oleksandr Kuznetsov, and Emanuele Frontoni. *Unrecognizable Yet Identifiable: Image Distortion with Preserved Embeddings*. 2024. arXiv: 2401.15048 [cs.CV].

[6] Dmytro Zakharov et al. *Embedding Non-Distortive Cancelable Face Template Generation*. 2024. arXiv: 2402.02540 [cs.CV].