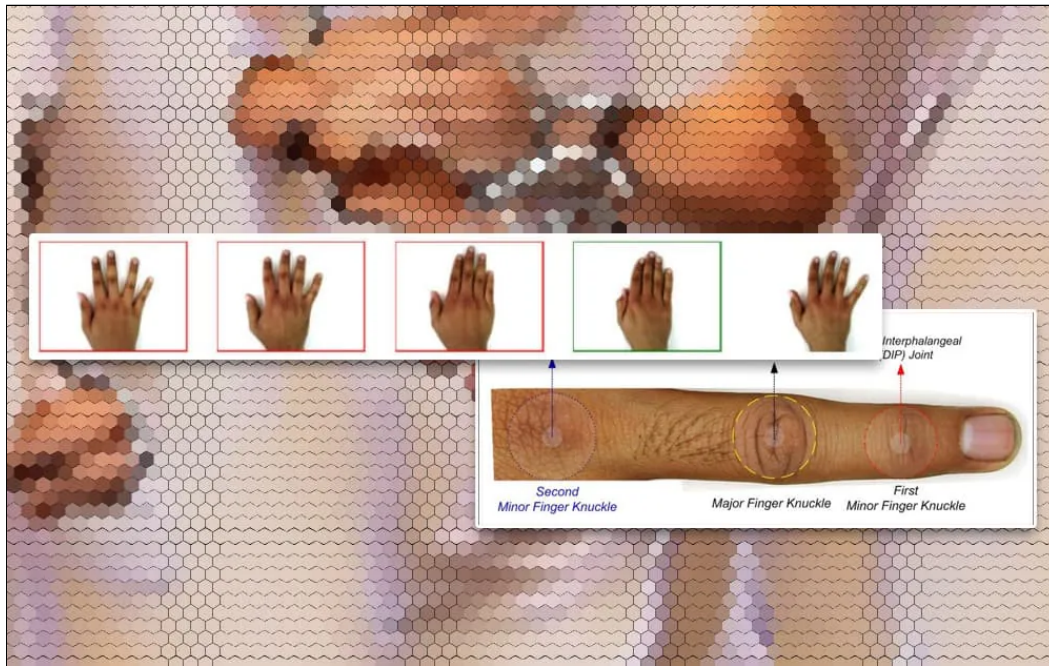


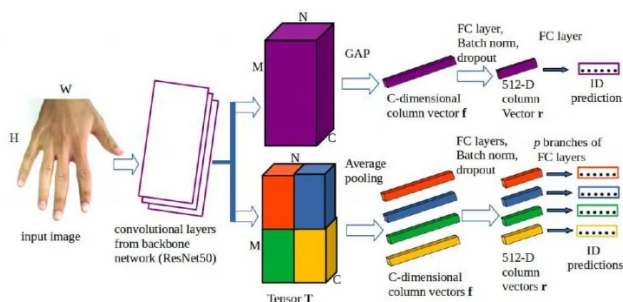
Using Hands as a Biometric Identifier in Criminal Video Forensics

Originally published at <https://www.unite.ai/using-hands-as-a-biometric-identifier-in-criminal-video-forensics/>



Researchers in the UK have developed a machine learning biometric system capable of identifying individuals from the shape of their hands. The intent of the work is to aid in identifying offenders, particularly in cases of sexual offenders that have recorded their crimes, where hand information is often the only biometric signal available.

The [paper](#), entitled *Hand-based Person Identification Using Global and Part-aware Deep Feature Representation Learning*, and proposes a new ML framework called Global and Part-Aware Network (GPA-Net).



In GPA-Net, two distinct 3D tensors (global and local) are obtained by passing the source image through stacked convolutional layers on the ResNet50 backbone network. Each of the analytical avenues will make an identity prediction. Source: <https://arxiv.org/pdf/2101.05260.pdf>

GPA-Net creates local and global branches on the convolutional layer, in order to create distinct recognition systems for both the entirety of the hands (with left and right hands distinctly recognized, unlike some previous attempts in this sector) and the *parts* of the hand, which in themselves can act as feeder flags for a better

identification of the whole hand.

The research comes from the School of Computing and Communications at Lancaster University, and is led by Nathanael L. Baisa, now an Assistant Professor at Leicester's De Montfort University.

Hands as Consistent Biometric Indicators

The researchers observe that hands offer a consistent collection of distinct biometric characteristics that can be [less subject](#) either to age, attempts at disguise, or other distorting factors (such as variation in expressions, in the case of facial capture) that can influence the reliability of more popular indicator systems, including gait recognition and facial recognition.

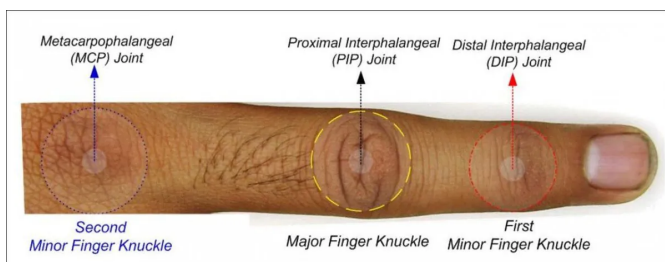
Though security systems have [been devised](#) that make use of hand vein patterns through infrared imaging, this is not likely to become available in the types of recording devices used in crimes. Rather, the current research concentrates on captures obtained through standard digital cameras, usually embedded in mobile devices, but in the case of sex crimes, often more likely to be obtained by 'dumb' cameras that are less inclined to share network information.

Ironically the palm print, possibly the most popular biometric method featured in science fiction movies of the last fifty years, has not enjoyed the uptake expected by futurists, perhaps because fingerprint ID systems require smaller and cheaper recognition surfaces. However, Fujitsu produced a [promotional study](#) in 2016 arguing that palm vein pattern recognition is a superior biometric tool for security systems.

Datasets and Testing

GPA-Net is, according to the researchers, the first end-to-end trained system to attempt hand recognition. The central backbone of its network is based on ResNet50 trained over ImageNet. These were chosen for their ability to perform well across a variety of platforms including [Google Inception](#) (a [GoogleNet](#) module that graduated to an evolving Convolutional Neural Network specializing in object detection and image analysis).

The GPA-Net framework was tested across two datasets – the 2016 [11k Hands](#) set, a collaboration between researchers from Canada and Egypt; and the Hong Kong Polytechnic University [Hand Dorsal \(HD\)](#) dataset.



A detail from 'Personal Identification Using Minor Knuckle Patterns From Palm Dorsal Surface', focusing on knuckle identification.

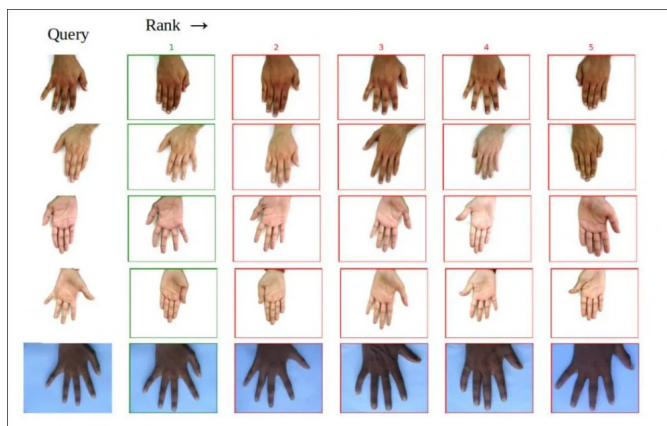
The 11k dataset features 190 identity subjects, including a variety of metadata regarding ID, age, skin color, gender, and other factors. The researchers excluded any images that contained jewelry, since these would inevitably end up as disruptive outliers. They also excluded images from the HD dataset that lacked adequate clarity, since ID matching is a more sensitive sector than image synthesis, and obscured data a greater danger.

GPA-Net was run on a PyTorch deep learning framework on a single NVIDIA GeForce RTX 2080 Ti GPU with 11gb of VRAM. The model was trained using [cross-entropy loss](#), and a mini-batch Stochastic Gradient Descent ([SGD](#)) optimizer. Training occurred over 60 epochs at an initial learning rate of 0.02, handled thereafter by a

learning rate scheduler with a decay factor of 0.1 for each 30 epochs – effectively slowing training down as high dimensional features quickly become embedded, and the system must subsequently spend longer traversing the data for more granular detail.

Evaluation was performed using the Cumulative Matching Characteristics ([CMC](#)) metric with Mean Average Precision (mAP).

The researchers found that GPA-Net outperforms competing methods on ResNet50 by 24.74% in rank-1 accuracy and by 37.82% on mAP.



Qualitative results from testing of the GPA-Net system. Top to bottom rows are the right dorsal recognitions of the 11k set, left dorsal of the same, right palmar of the same, and the left palmar of the 11k and HD datasets. Green and red bounding boxes indicate correct and incorrect matches.

The researchers consider that the method has ‘strong potential for robust identification of the perpetrators of serious crime’.

Writer on machine learning, domain specialist in human image synthesis. Former head of research content at Metaphysic.ai, until its dissolution into DNEG's Brahma.ai.

Portfolio site: martinanderson.ai

Contact: martin@martinanderson.ai



Discover More