**Reference**
10117

**Inventor(s)**
Dr. George Shaker

**Patent status**
US patent pending

**Stage of development**
Prototype
Ongoing research

**Contact**
Scott Inwood
Director of Commercialization
Waterloo Commercialization Office
519-888-4567, ext. 33728
sinwood@uwaterloo.ca
uwaterloo.ca/research

## Fingerprint biometric identification utilizing millimetre waves

## Background

Biometrics offer a personal and convenient way of keeping our identities and our data secure. There are many biometric authentication methods that have been extensively studied, ranging from fingerprint scanners to retina sensors to facial recognition software. Of all of these, fingerprinting is likely the most well-known, and has been achieved through a wide variety of methods, whether based on infrared, multiple camera systems, or on acoustic waves. However, all of these have been shown to be prone to skimming and identity theft. In most of such cases, criminals can create a 3D printed finger or hand with identical features to those of a user finger or hand when exposed to the aforementioned fingerprint scanners.

## Description of the invention

A method of using wireless waves to identify various individuals has been developed. In this system, the compact transceiver has a number of transmit and receiver antennas. The transmitter(s) send a sequence of signals which are absorbed, reflected, and scattered from a nearby part of the body of a user (a hand in our demo case) and the resulting signal is detected at a receiver(s) antenna. Different signal processing algorithms are applied to the received signals in order to create a rich feature dataset. The resulting dataset is classified using machine learning models, which are shown to facilitate identifying a group of individuals with high accuracy.

## Advantages

This technology has promising applications as an independent or an auxiliary tool for biometric authentication. The technology promises to be of a much higher level of security and immunity against identity thefts and hacking attempts than existing technologies.

## Potential applications

- Border Control/Airports.
- Military Security Systems.
- Voter registration and identification.
- Banking and Purchase Authentication.
- Smartphone and Laptop Access.
- Household Door Locks.
- Logical Access Control.
- Secure Health Records Access.
- Time and attendance Records.
- Falls detection (hospitals, home use, etc)