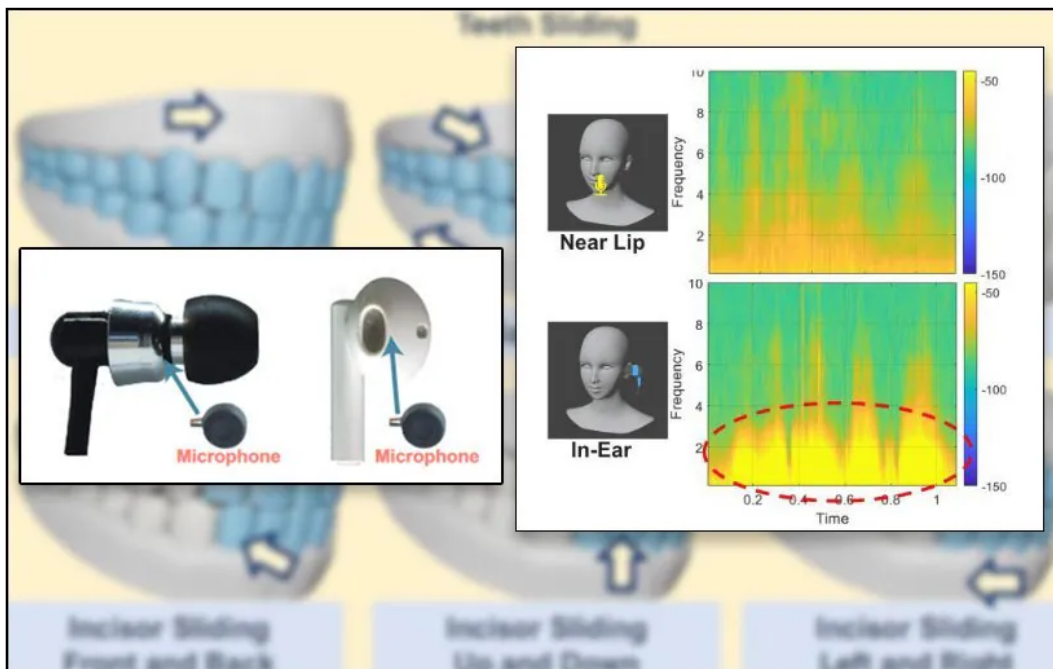
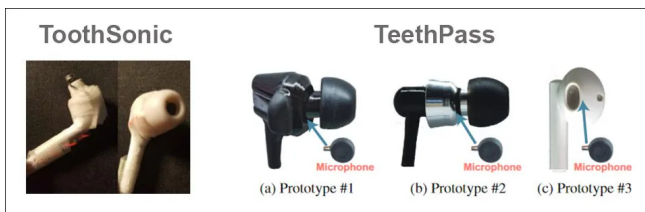


Biometric Authentication by Grinding Your Teeth

Originally published at <https://www.unite.ai/biometric-authentication-by-grinding-your-teeth/>



Two recent research papers from the US and China have proposed a novel solution for teeth-based authentication: just grind or bite your teeth a bit, and an ear-worn device (an 'earable', that may also double up as a regular audio listening device) will recognize the unique aural pattern produced by abrading your dental architecture, and generate a valid biometric 'pass' to a suitably equipped challenge system.



Various ear-worn prototype devices for the two systems. Sources: <https://arxiv.org/ftp/arxiv/papers/2204/2204.07199.pdf> (ToothSonic) and <https://cis.temple.edu/~yu/research/TeethPass-Info22.pdf> (TeethPass)

Prior methods of dental authentication (i.e. for living people, rather than forensic identification), have needed the user to 'grin and bare', so that a dental recognition system could confirm that their teeth matched biometric records. In summer of 2021, a research group from India made headlines with such a system, [titled DeepTeeth](#).

The new proposed systems, dubbed *ToothSonic* and *TeethPass*, come respectively from an academic collaboration between Florida State University and Rutgers University in the United States; and a joint effort between researchers at Beijing Institute of Technology, Tsinghua University, and Beijing University of Technology, working with the Department of Computer and Information Sciences at Temple University in Philadelphia.

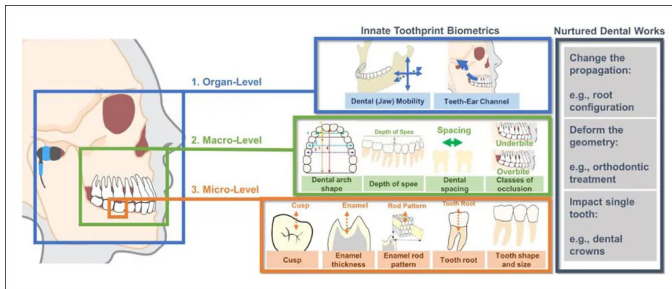
ToothSonic

The entirely US-based ToothSonic system has been proposed in the [paper](#) *Ear Wearable (Eearable) User Authentication via Acoustic Toothprint*.

The ToothSonic authors state:

'ToothSonic [leverages] the toothprint-induced sonic effect produced by users performing teeth gestures for earable authentication. In particular, we design representative teeth gestures that can produce effective sonic waves carrying the information of the toothprint.'

'To reliably capture the acoustic toothprint, it leverages the occlusion effect of the ear canal and the inward-facing microphone of the earables. It then extracts multi-level acoustic features to reflect the intrinsic toothprint information for authentication.'



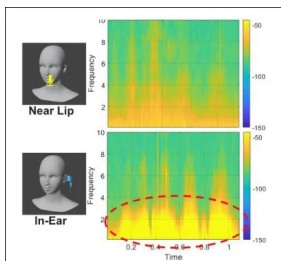
Contributing impact factors that formulate a unique aural toothprint registered in an ear-worn device. Source: <https://arxiv.org/ftp/arxiv/papers/2204/2204.07199.pdf>

The researchers note a number of advantages of aural tooth/skull signature patterns, which also apply to the primarily Chinese project. For instance, it would be extraordinarily challenging to mimic or spoof the toothprint, which must travel through the unique architecture of the head tissues and skull channel before arriving at a recordable 'template' against which future authentications would be tested.

Additionally, toothprint-based identification not only eliminates the potential embarrassment of grinning or grimacing for a mobile or mounted camera, but removes the need for the user to in any way distract themselves from potentially critical activities such as operating vehicles.

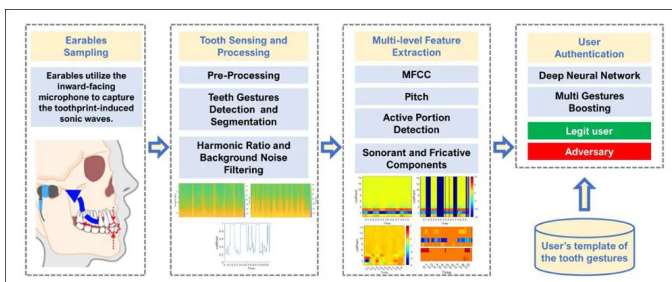
Besides this, the method is suitable for many people with motor impairments, while the devices can potentially be incorporated into earbuds whose primary usage is far more common (i.e. listening to music and making telephone calls), removing the need for dedicated, standalone authentication devices, or recourse to mobile applications.

Further, the possibility of reproducing a person's dentition in a spoof attack (i.e. by printing a photo from an uninhibited social media photo post), or even replicating their teeth in the unlikely scenario of obtaining complex and complete dental molds, is obviated by the fact the sounds abrading teeth make are filtered through completely hidden internal geometry of the jaw and the auditory canal.



From the ToothSonic paper, the occluding effect of the ear canal makes casual reproduction or imitation effectively impossible.

As an attack vector, the only remaining opportunity (besides forcible and physical coercion of the user) is to gain database access to the host security system and entirely substitute the user's recorded aural tooth pattern with the attacker's own pattern (since illicitly obtaining somebody else's toothprint would not lead to any practical method of authentication).



Workflow for ToothSonic.

Though there is a tiny opportunity for an attacker to playback a recording of the mastication in their own mouths, the Chinese-led project found that this is not only a conspicuous but very ill-starred approach, with minimal chance of success (see below).

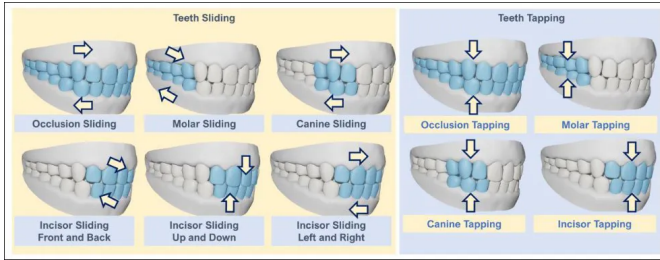
A Unique Smile

The ToothSonic paper outlines the many unique characteristics in a user's dentition, including classes of occlusion (such as overbite), enamel density and resonance, missing aural information from extracted teeth, unique characteristics of porcelain and metal substitutions (among other possible materials), and cusp morphology, among many other possible distinguishing features.

The authors state:

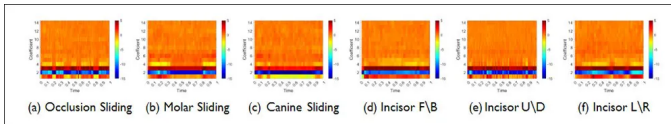
'[The] toothprint-induced sonic waves are captured via the user's private teeth-ear channel. Our system thus is resistant to advanced mimic and replay attacks as the user's private teeth-ear channel secures the sonic waves, which are unlikely uncovered by adversaries.'

Since jaw movement has a limited range of mobility, the authors envisage ten possible manipulations that could be recorded as viable biometric prints, illustrated below as 'advanced teeth gestures':



Some of these movements are more difficult to achieve than others, though the more difficult movements do not result in patterns that are any more or less easy to replicate or spoof than less challenging movements.

Macro-level characteristics of apposite teeth movements are extracted using a [Gaussian mixture model](#) (GMM) speaker identification system. Mel-frequency cepstral coefficients ([MFCCs](#)), a representation of sound, are obtained for each of the possible movements.



Six different sliding gestures for the same subject during MFCC extraction under the ToothSonic system.

The resulting signature sonic wave that comprises the unique biometric signature is highly vulnerable to certain human body vibrations; therefore ToothSonic imposes a filter band between 20-8000Hz.

Sonic wave segmentation is achieved via a Hidden Markov Model ([HMM](#)), in accordance with two prior [works](#) from Germany.

For the authentication model, derived features are fed into a fully connected neural network, traversing various layers until activation via [ReLU](#). The last fully connected layer uses a Softmax function to generate the results and predicted label for an authentication scenario.

The training database was obtained by asking 25 participants (10 female, 15 male) to wear an adulterated earbud in real-world environments, and conducting their normal activities. The prototype earbud (see first image above) was created at a cost of a few dollars with off-the-shelf consumer hardware, and features one microphone chip. The researchers contend that a commercial implementation of such as device would be eminently affordable to produce.

The learning model comprised the neural network classifiers in MATLAB, trained at a learning rate of 0.01, with [LBFGS](#) as the loss function. Evaluation methods for authentication were [FRR](#), [FAR](#) and [BAC](#).

Overall performance for ToothSonic was very good, depending on the difficulty of the internal mouth gesture being performed:



Results were obtained across three grades of difficulty of mouth gesture: *comfortable*, *less comfortable*, and *have difficulties*. One of the user's preferred gestures achieved an accuracy rate of 95%.

In terms of limitations, the users concede that changes in teeth over time will likely require a user to re-imprint the aural tooth signature, for instance after notable dental work. Additionally, enamel quality can degrade or otherwise change over time, and the researchers suggest that older people might be asked to update their profiles periodically.

The authors also concede that multi-use earbuds of this nature would require the user to pause music or conversation during authentication (in common with the Chinese-led TeethPass), and that many currently available earbuds do not have the necessary computational power to facilitate such as system.

In spite of this, they observe*:

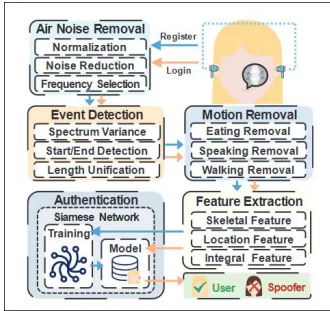
'Encouragingly, recent releases of the Apple H1 chip in the AirPods Pro and QCS400 by Qualcomm are capable to support voice-based on-device AI. It implies that implementing ToothSonic on earable could be realized in near future.'

However, the paper concedes that this additional processing could impact battery life.

TeethPass

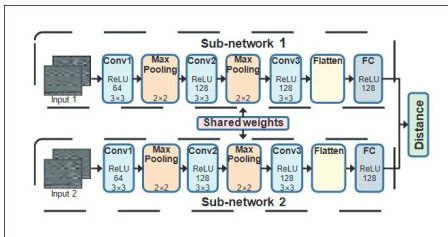
Released in the [paper](#) *TeethPass: Dental Occlusion-based User Authentication via In-ear Acoustic Sensing*, The Chinese-American project operates on much the same general principles as ToothSonic, accounting for the traversal of signature audio from dental abrasion through the auditory canal and intervening bone structures.

Air noise removal is conducted at the data gathering stage, combined with noise reduction and – as with the ToothSonic approach – an appropriate frequency filter is imposed for the aural signature.



System architecture for TeethPass.

The final extracted MFCC features are used to train a [Siamese neural network](#).



Structure of the Siamese neural network for TeethPass.

Evaluation metrics for the system were FRR, FAR, and a confusion matrix. As with ToothSonic, the system was found to be robust to three types of possible attack: mimicry, replay, and hybrid attack. In one instance, the researchers attempted an attack by playing the sound of a user's dental movement inside the mouth of an attacker, with a small speaker, and found that at distances less than 20cm, this hybrid attack method has a higher than 1% chance of success.

In all other scenarios, the obstacle of mimicking the target's inner skull construction, for instance during a replay attack, makes a 'hijacking' scenario among the least likely risk in the standard run of biometric authentication frameworks.

Extensive experiments demonstrated that TeethPass achieved an average authentication accuracy of 98.6%, and could resist 98.9% of spoofing attacks.

* My conversion of the authors' inline citation/s to hyperlink/s

First published 18th April 2022. Updated 19th April 8:30am EET to correct package misattributions in captions.

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