Brain Hacking: Assessing Psychological and Computational Vulnerabilities in Brain-Based Biometrics

PIs: Zhanpeng Jin and Wenyao Xu, University at Buffalo

NSF SaTC #1840790/1564104

Project URL: https://cybermed.cse.buffalo.edu/wiki/index.php/BrainHacking

Motivation

Brainprints, like other biometrics, may be possible to circumvent — which may cause security vulnerability.

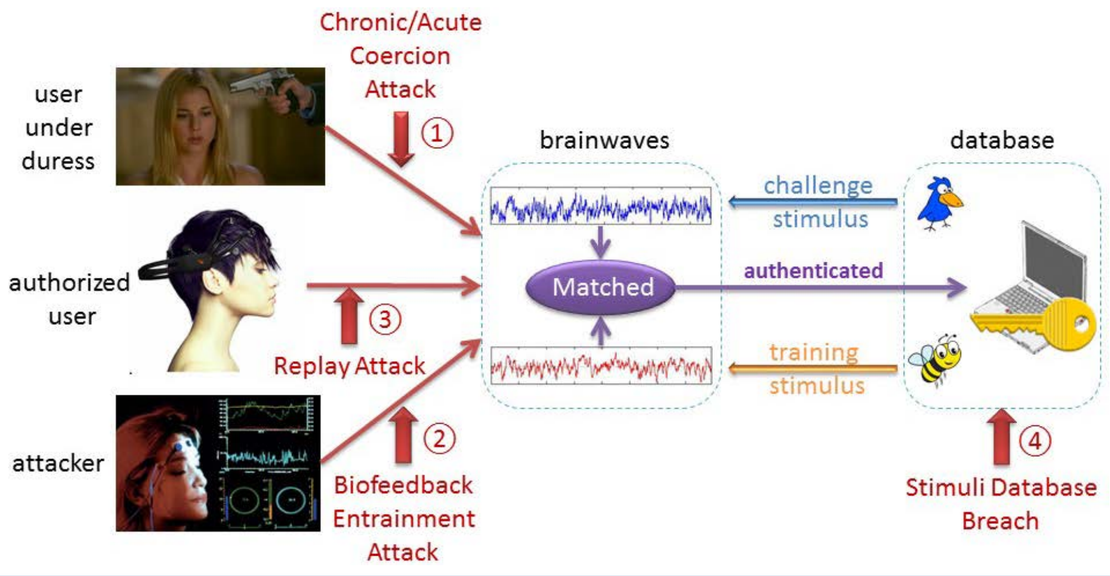
The objective is to systematically and comprehensively investigate the vulnerabilities and resistance of brainprint biometrics to psychological and computational attacks.

Psychological Vulnerabilities: Feasibility of impersonating a brainprint via biofeedback. Resistance of the braintprint to being elicited under duress.

Computational Vulnerabilities: fake or falsified biometric trait and compromised biometric templates.

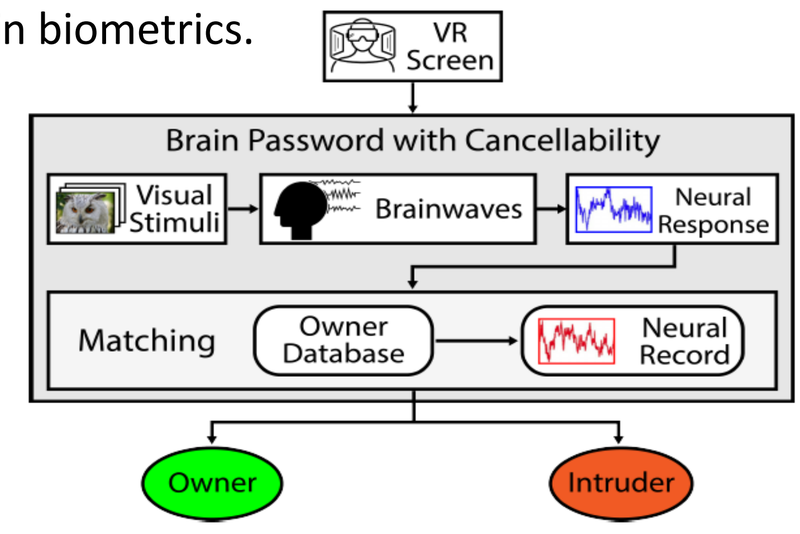
Attack Models

- Chronic/Acute Coercion Attack
- Biofeedback Entrainment Attack
- Replay/Presentation Attack
- Stimuli Database Attack

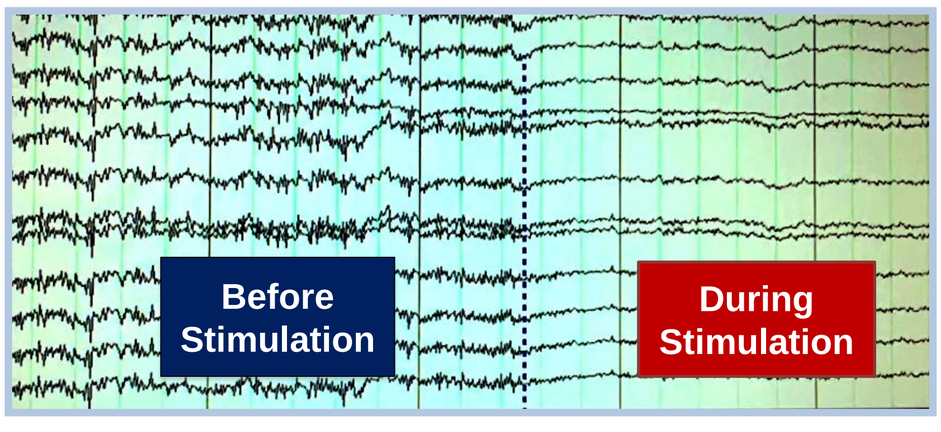


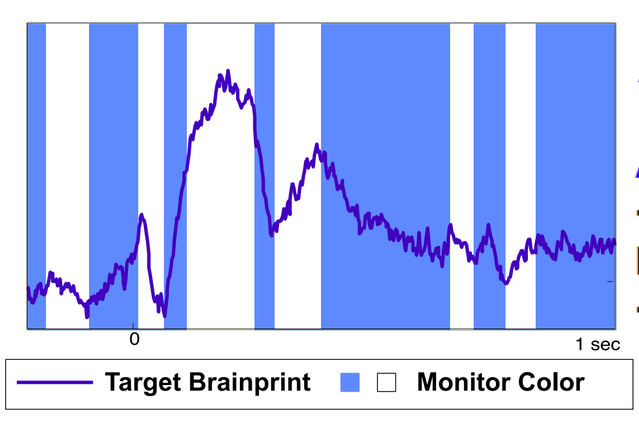
Methods

- New residue-based deep learning techniques for detecting fake brainwaves
- Brainprint impersonation under various brainwave entrainment schemes.
- Brainprint updating for truly cancelable (replaceable) brain biometrics.



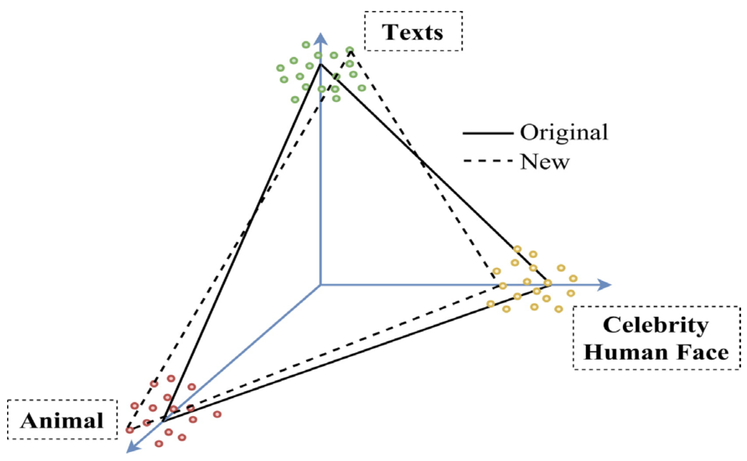
Psychological Entrainment Attack

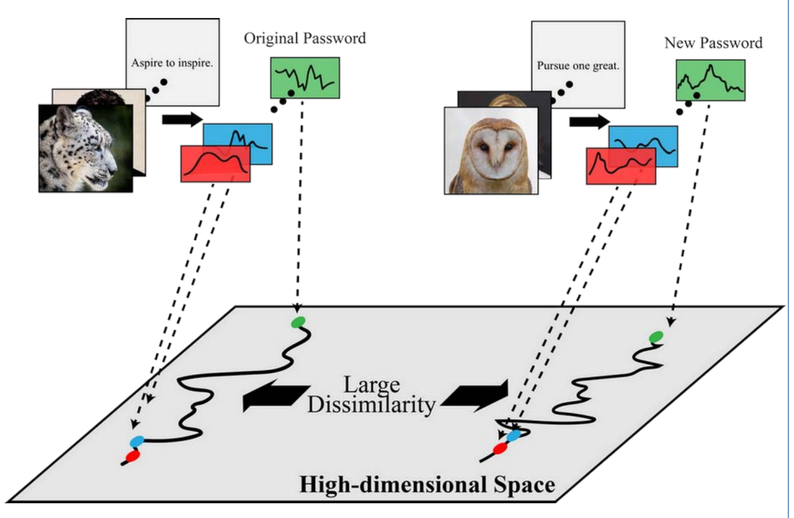




Visually Evoked Brainprint Updating

Spatio-Temporal Warping Distance





Revocability: new ERP distinguishable from others
Unlinkability: new ERP unlinkable to the old one

Broader Impact

- This research helps the community understand what is and is not possible to do to attack a brain biometric.
- Substantial popular media attention on this project brings it to a wide audience.
- Makes the public aware of that biometrics aren't foolproof.
- Aids in the design of brain biometrics outside the lab.