Exploring Vulnerabilities of Brain Biometrics

PIs: Zhanpeng Jin and Sarah Laszlo (SUNY-Binghamton), Wenyao Xu (SUNY-Buffalo)

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
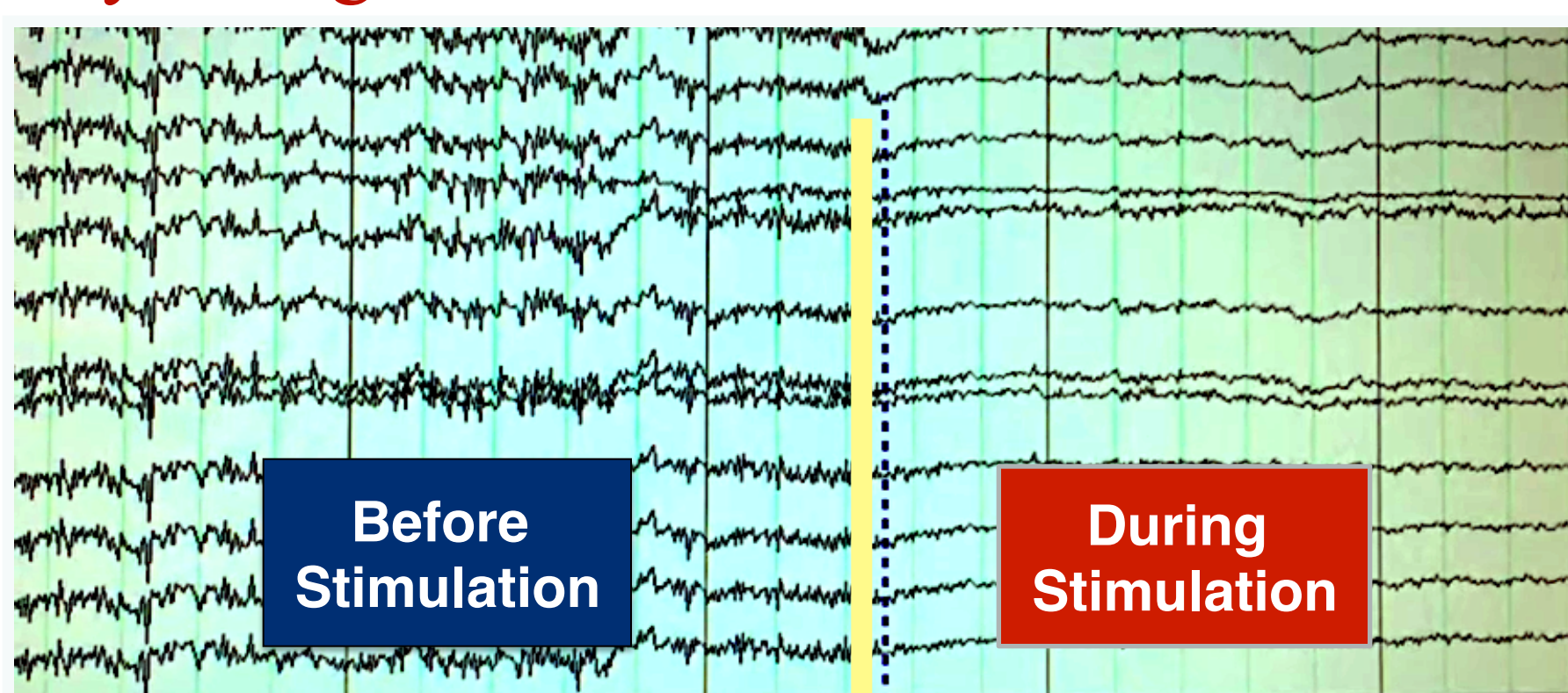- Stimuli Database Attack
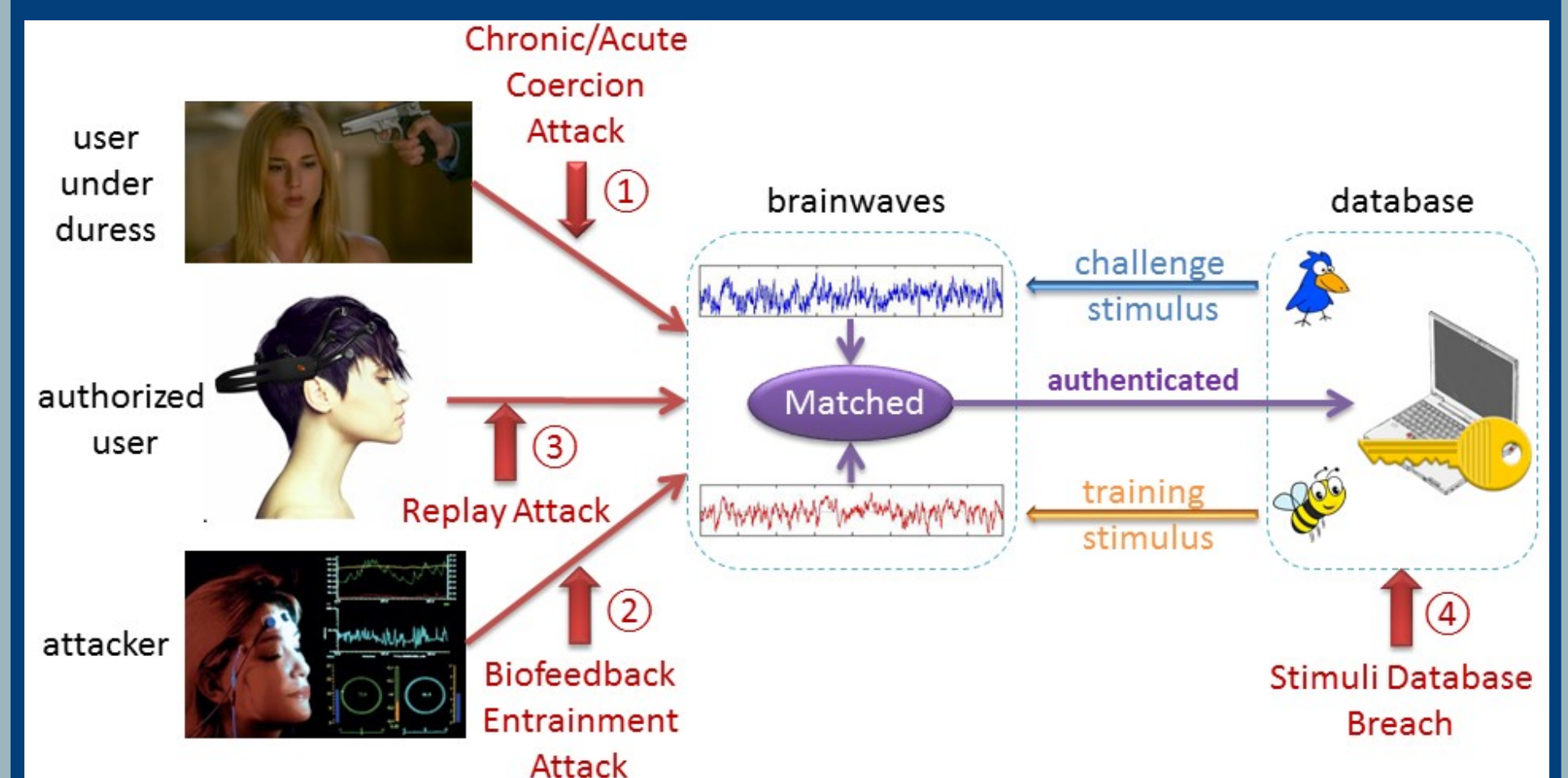
Approaches

Psychological Coercion Attacks

- Blackmail-type chronic coercion
- Threat-of-violence-type acute coercion
- Rationale: Forms of coercion that place psychological stress on the user may cause brain activity to deflect

Computational Attacks

Psychological Entrainment Attack

Before Stimulation   During Stimulation
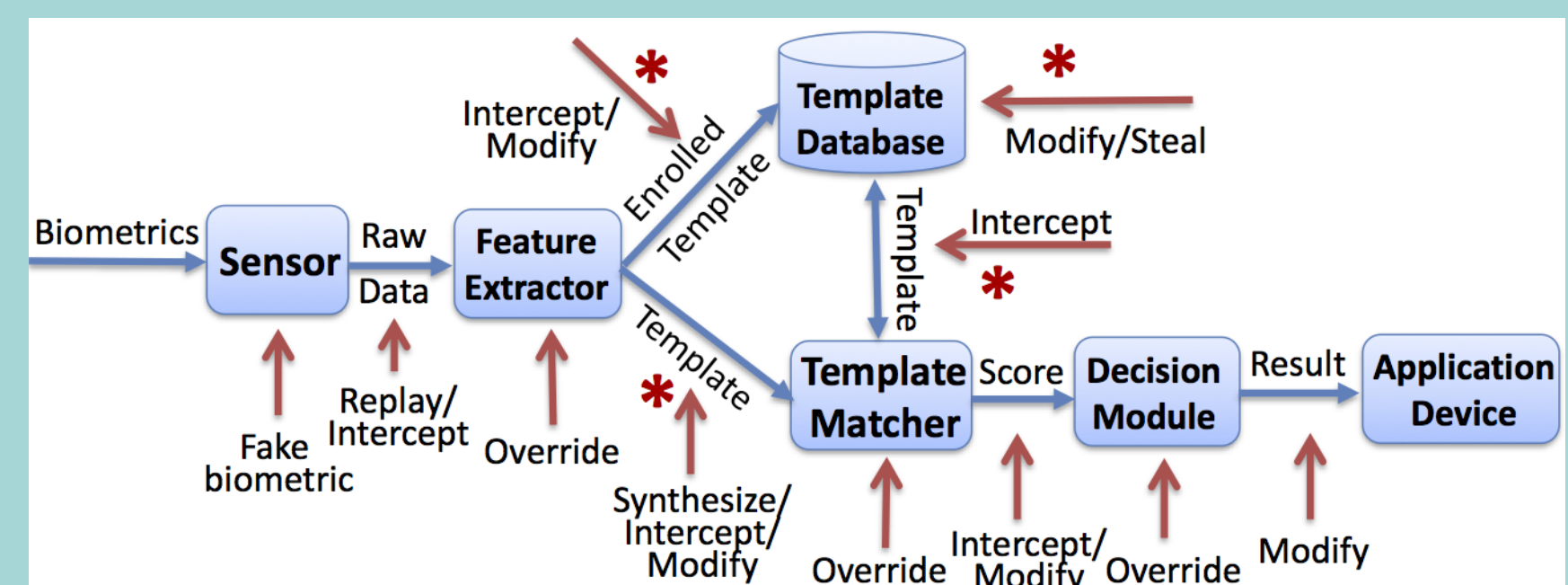
Noise Residual Feature
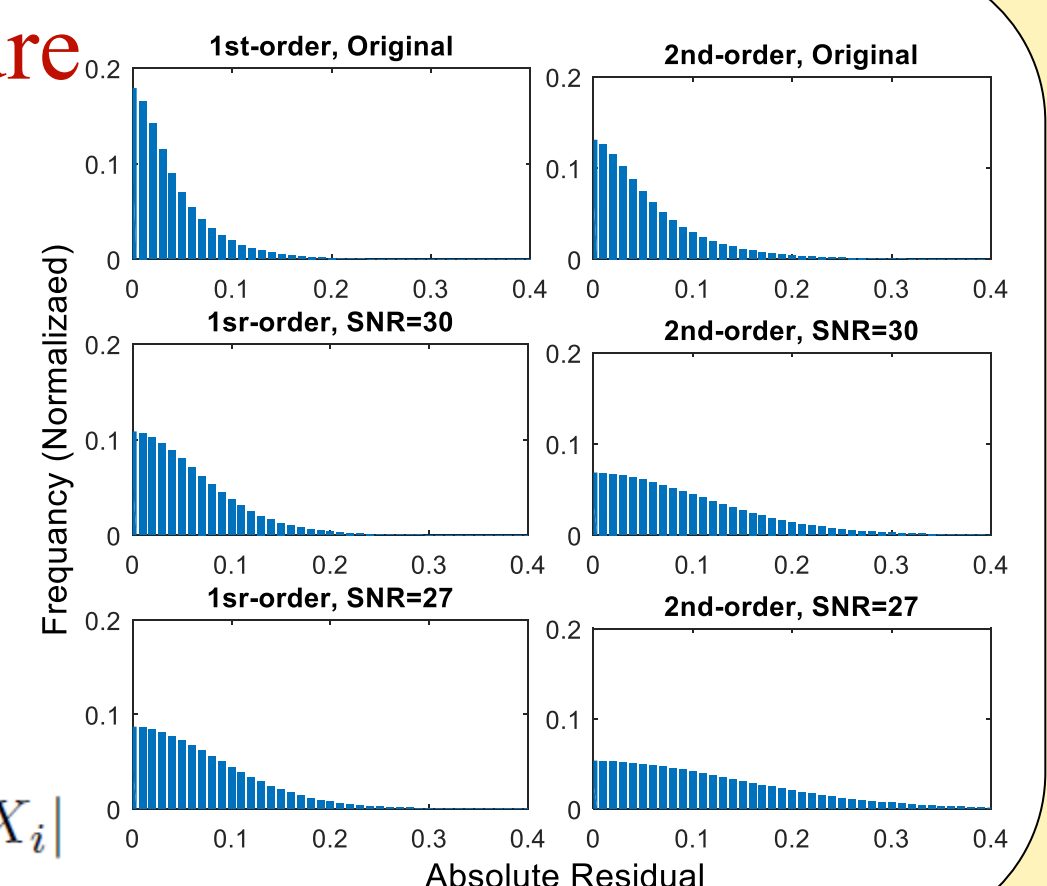
Noise Residuals

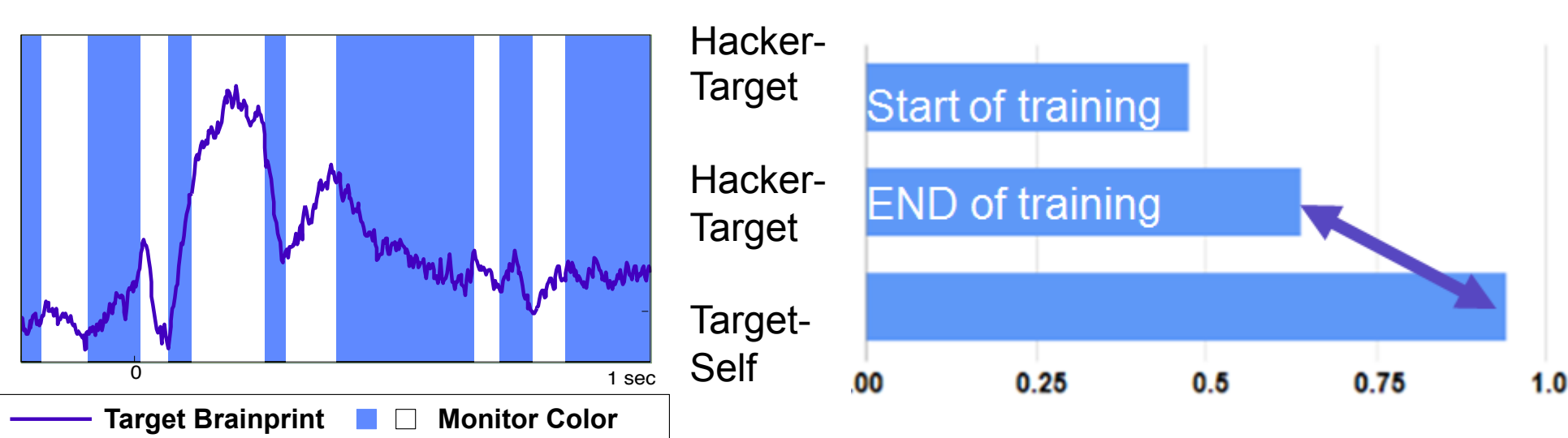$$\mathbf{R_c(i)} = |\hat{X}_i(\mathcal{N}_i) - cX_i|$$

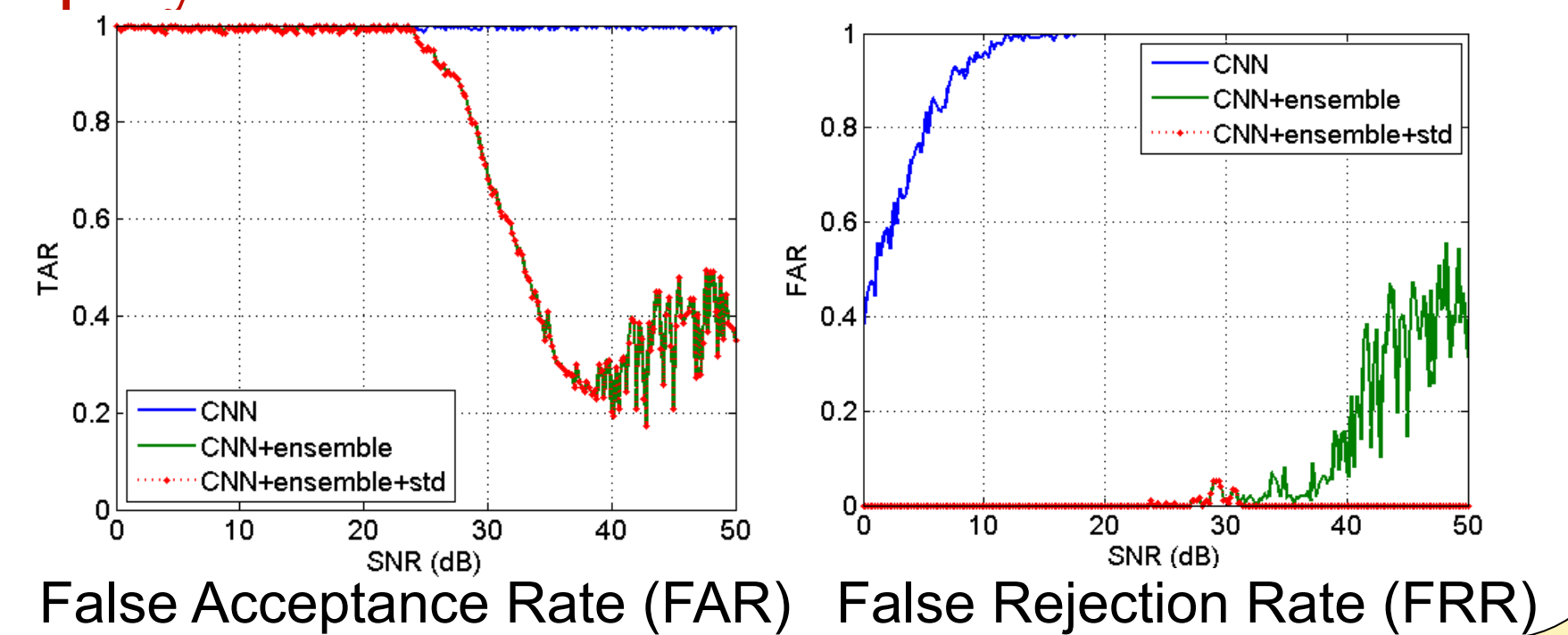1st-order Residuals

$$\mathbf{R_1(i)} = |X_{i+1} - X_i|$$

2nd-order Residuals

$$\mathbf{R_2(i)} = |X_{i-1} + X_{i+1} - 2X_i|$$

Psychological Entrainment Attack

Hacker-Target — Start of training
Hacker-Target — END of training
Target-Self

Replay Attack Detector

False Acceptance Rate (FAR)   False Rejection Rate (FRR)

Interested in meeting the PIs? Attach post-it note below!

National Science Foundation — WHERE DISCOVERIES BEGIN

BINGHAMTON UNIVERSITY — STATE UNIVERSITY OF NEW YORK

University at Buffalo — The State University of New York