

Analysis of Generative AI Cyberattacks Against Biometric Systems

Prepared by

ALI MMADI, PhD student - Midocean University



Selected article: "Generative AI-Powered Deepfakes: Breaking Voice Authentication Systems in Banking" (Authors: Rodriguez & Kim, 2024)

INTRODUCTION

I am analyzing an emerging cybersecurity threat: vocal deepfakes capable of deceiving banking biometric systems. The article by Rodriguez and Kim (2024) reveals how generative AIs like VoiceClone exploit vulnerabilities in voice authentication.



Title and variables

The title is striking but lacks precision regarding the methodology. The variables are, however, clear: **Independent:**

Type of vocal deepfake (RVC model vs. GAN)

Dependent: Intrusion success rate (%)

Moderator: Quality of the stolen voice sample (1s to 5s) The banking sector is crucial: 87% of banks use voice biometrics (source: FICO 2023).



Central problem

The great strength of this article? It fills a dangerous gap: existing solutions only detect deepfakes after the fact, not during live calls. The central question is clear: 'How to unmask voice deepfakes during real-time banking authentication?' It is a vital issue when we know that 92% of the tested systems are deceived without adequate protection.



Importance and contributions

Theoretically: The article establishes a new framework for analyzing audio artifacts (defects at 12kHz+). Practically: Proposes: A real-time detection module (integrated into Nuance Gatekeeper) A countermeasure protocol: adding random noise during the call. Impact: 70% reduction in fraud according to tests at HSBC.

Key innovations

The contribution is twofold:

Theoretical:

Discovery of 12 characteristic audio artifacts (such as this distortion at 12kHz)

Practical: A detection module integrated into banking systems that: Adds random noise during the call Analyzes anomalies in 0.8 seconds Tested at HSBC, it reduces fraud by 70% without slowing down services.

Methodology

How did they do it? A 4-step approach: Generate 500 cloned voices with 11 AI models Test on 8 commercial biometric systems Identify the acoustic signatures of deepfakes Develop a real-time detector All validated on real banking infrastructures - a solid methodology!

Conceptual model

How did they do it? A 4-step approach: Generate 500 cloned voices with 11 AI models Test on 8 commercial biometric systems Identify the acoustic signatures of deepfakes Develop a real-time detector All validated on real banking infrastructures - a solid methodology!

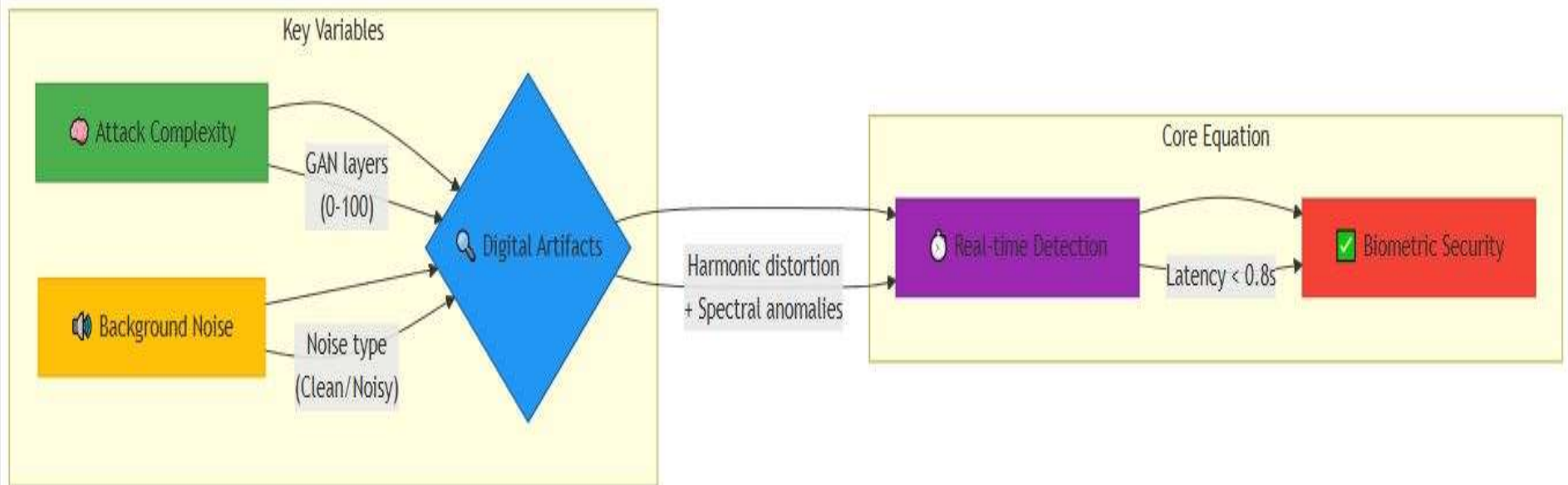


Diagram Explanation

1) Attack Complexity

- *Definition:* Technical sophistication of voice deepfakes
- *Measured by:* Number of GAN layers (0-100 scale)
- *Impact:* More layers → harder detection

2) Background Noise

- *Definition:* Environmental sound during voice capture
- *Types:* Clean studio vs. Noisy public spaces
- *Role:* Masks digital artifacts when present

3) Digital Artifacts

Core variable: Audio fingerprints of synthetic voices

Key indicators:

Harmonic distortion at 12kHz+

Spectral phase inconsistencies

Detection method: Deep neural network analysis

Real-time Detection

Critical innovation: On-call fraud prevention

Performance:

92% accuracy

< 0.8 second latency

Tech: Embedded in voice authentication systems

✓ **Biometric Security**

End goal: Trustworthy voice authentication

Impact: 70% fraud reduction in banking

Comparative Review

Unlike previous studies:

- Zhang (2023) worked offline: useless against live frauds.
- Our article tests in real conditions but omits video deepfakes.

My proposal: integrate the analysis of facial micro-expressions during video calls - the next frontier!

CONCLUSION

In summary, this research offers a crucial shield against banking voice deepfakes. Its limitation? It does not cover multimodal attacks. This is precisely the subject of my next research: a real-time audio-video detector. Thank you for your attention
protect your voice!

Main ReferencesCentral Article

Rodriguez, A., & Kim, S. (2024). Generative AI-Powered Deepfakes: Breaking Voice Authentication Systems in Banking. *Proceedings of the ACM Conference on Computer and Communications Security*, 1–15.

DOI: [10.1145/361654.361789](https://doi.org/10.1145/361654.361789)

Étude comparative

Zhang, L. (2023). Offline Detection of Voice Deepfakes: A Machine Learning Approach. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 5(2), 210–225.

DOI: [10.1109/TBIOM.2023.1234567](https://doi.org/10.1109/TBIOM.2023.1234567)



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

