



„Niekonwencjonalne luki cyberbezpieczeństwa - nieautoryzowana rekonstrukcja sygnałów poprzez techniki bioakustyczne, optyczne ”

mgr inż. Katarzyna Pietrzak
dr inż. Wojciech Wodo
Politechnika Wrocławska



Główny cel:

empiryczna weryfikacja wykonalności 3
niekonwencjonalnych ataków kanałem bocznym
(zbudowanie autorskich stanowisk pomiarowych DIY)

Trzy obszary badawcze:

- **Bioakustyka** - Implant wywiadowczy w tkance zwierzęcej (symulacja)
- **Optyka** - Mikrofon wizualny (analiza drgań obiektu z wideo 240 FPS)
- **Elektrodynamika** - Retasking głośnika w mikrofon (przebudowa toru audio)

Konstrukcja makiety DIY:

- żel balistyczny
- kości drobiowe
- lisia skóra

Pomiary w środowisku:

- wewnętrznym
- zewnętrznym

Testowane sygnały:

- tonalne (1 kHz)
- ciągłe (Chirp 50 Hz – 10 kHz)
- naturalna rozmowa ludzka

Głębokość:

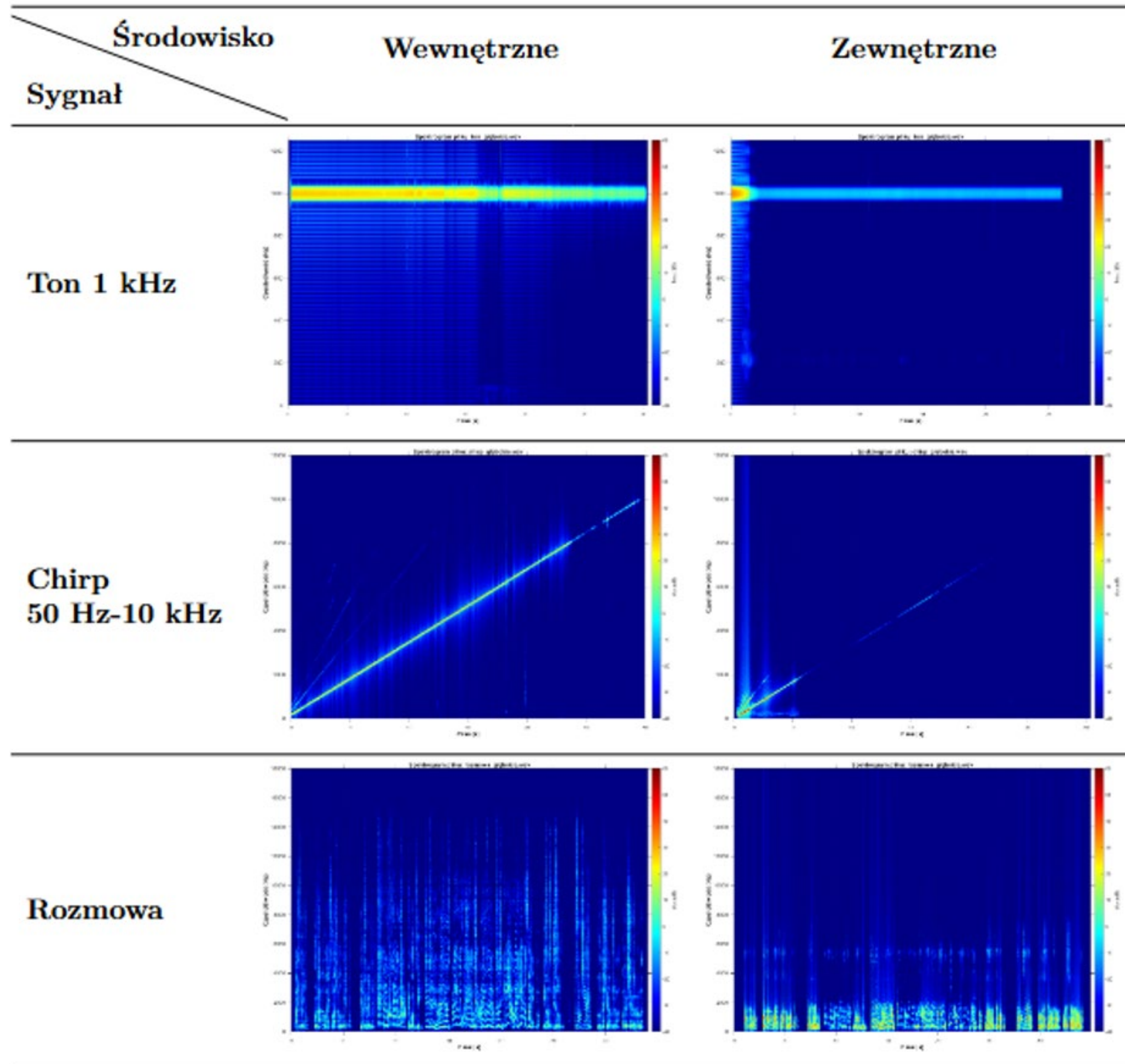
- implementacja podskórna
- intermuskularna (głęboka)



Kluczowy sukces:
uzyskanie wyraźnej, czytelnej mowy
ludzkiej z odległości **aż 6 metrów** od
makiety (nawet w warunkach
zewnętrznych!).

Optymalna głębokość:
implementacja intermuskularna tłumi
szumy otoczenia najlepiej, zachowując
czytelność sygnału.

Wniosek dla IT/IoT:
dowód na fizyczną wykonalność
mikrouządzeń wywiadowczych (np.
MEMS) ukrytych w środowisku bio-
fizycznym.



Koncepcja:

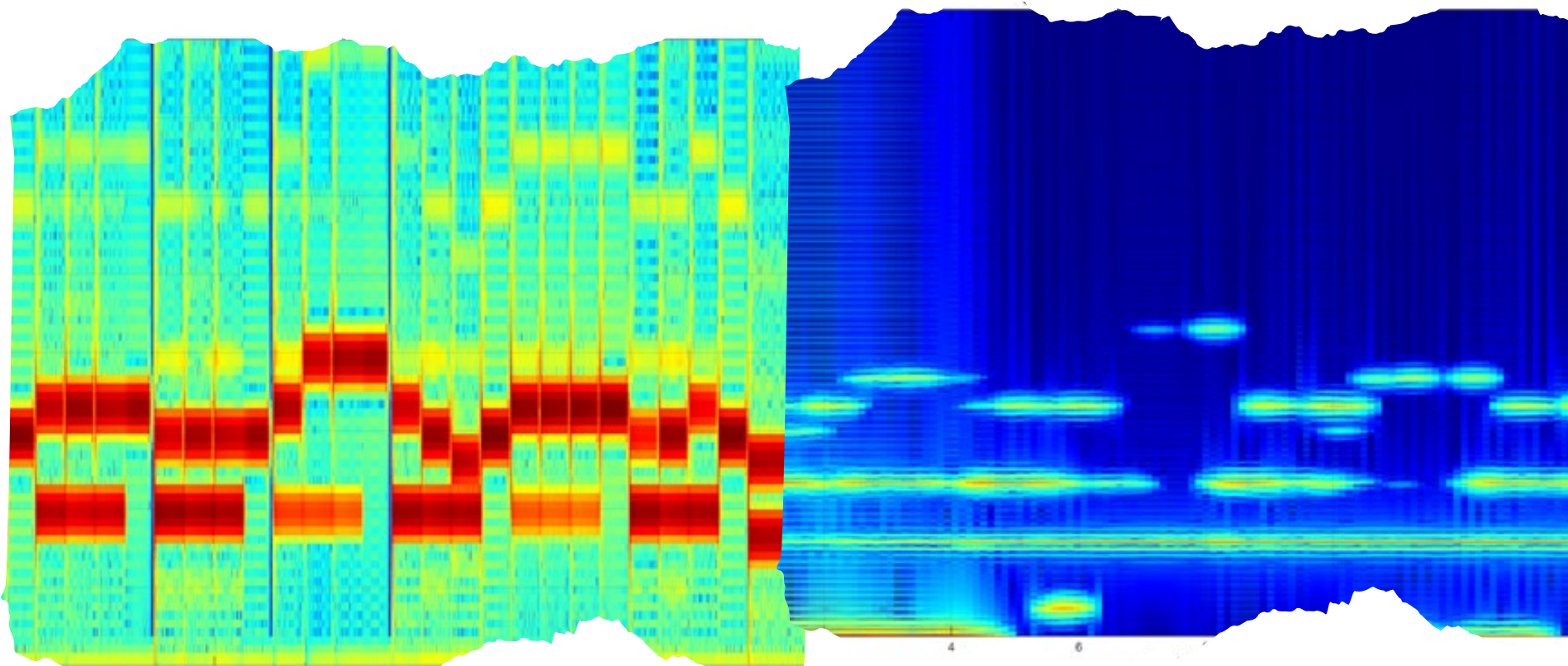
Pasywny odczyt mikrodchyleń obiektu (paczka chipsów) wywołanych falą akustyczną przy użyciu wideo.

Stanowisko pomiarowe:

Smartfon (Slow Motion 240 FPS)
jednorodne oświetlenie
głośnik testowy.

Algorytmika:

Matematyczna dekompozycja obrazu



Wynik eksperymentu:

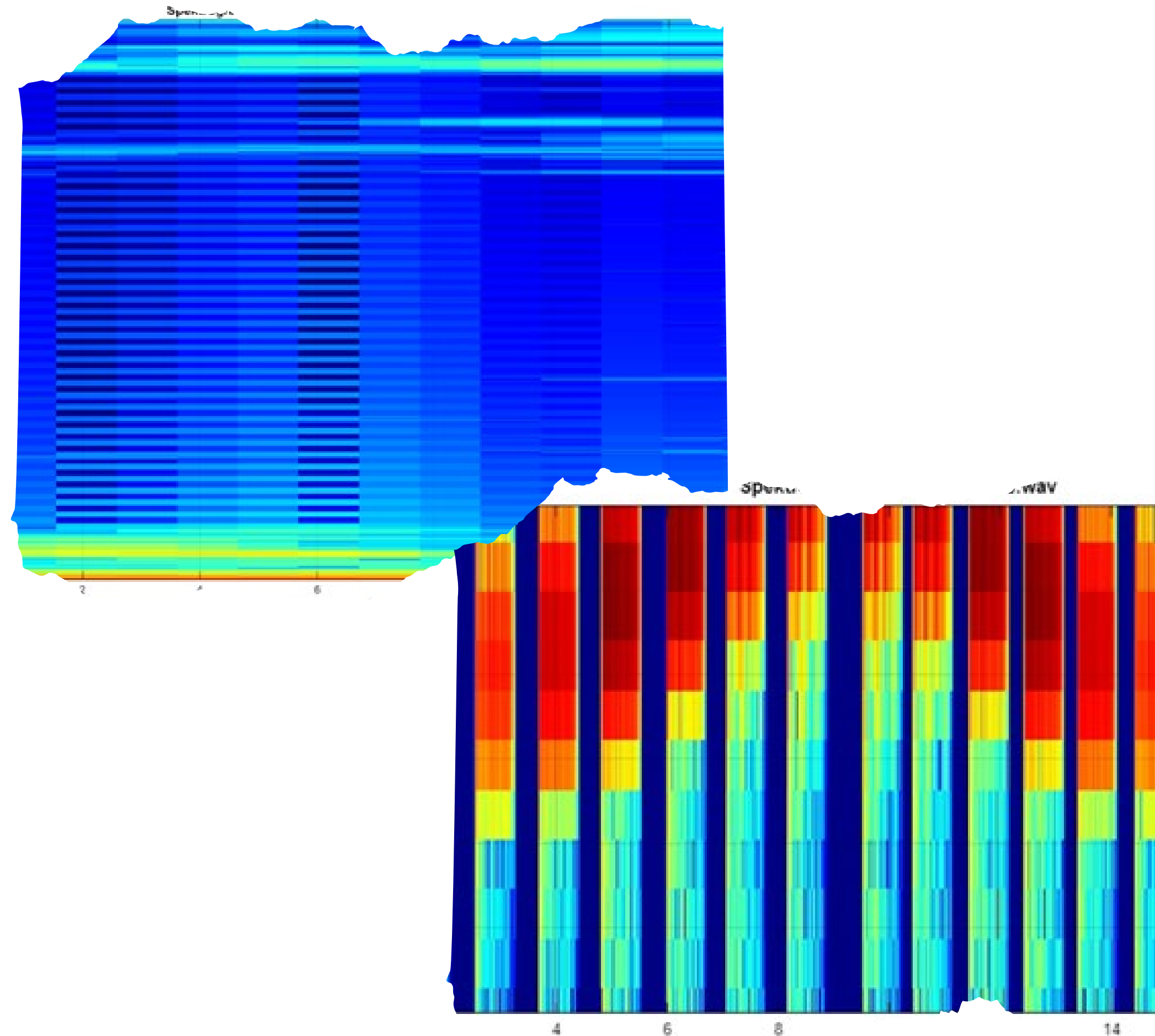
Potwierdzenie poprawności pipeline'u matematycznego, ale brak możliwości odzyskania czytelnego dźwięku z kamery smartfona - 240 FPS.

Przyczyna:

Limit Shannona-Nyquista — częstotliwość klatkowania 240 FPS jest zbyt niska dla złożonych częstotliwości audio.

Wektor rozwoju:

Potencjał wykorzystania wskaźników laserowych (interferometria) lub własnych mikrosystemów wizyjnych high-FPS.

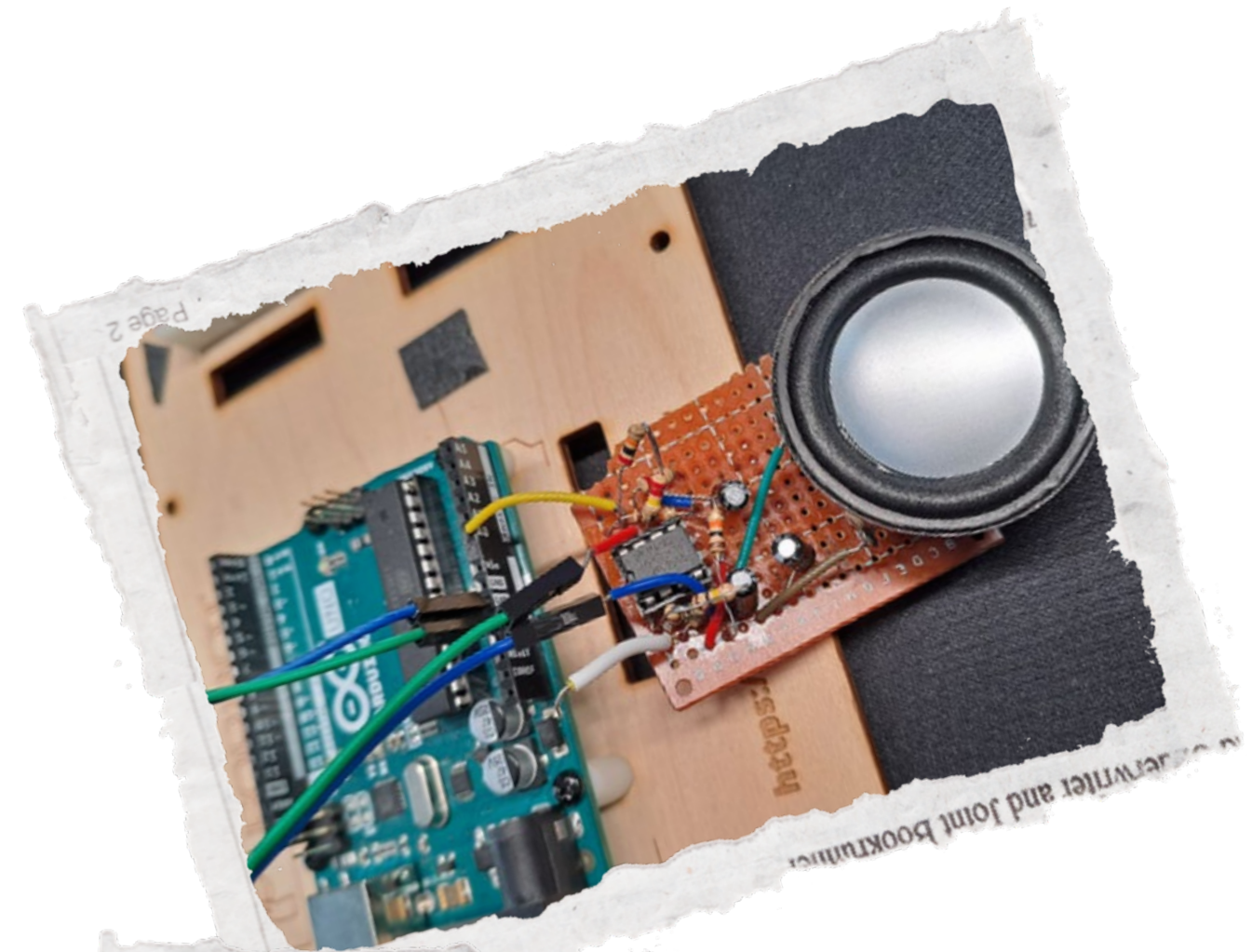


Koncepcja:

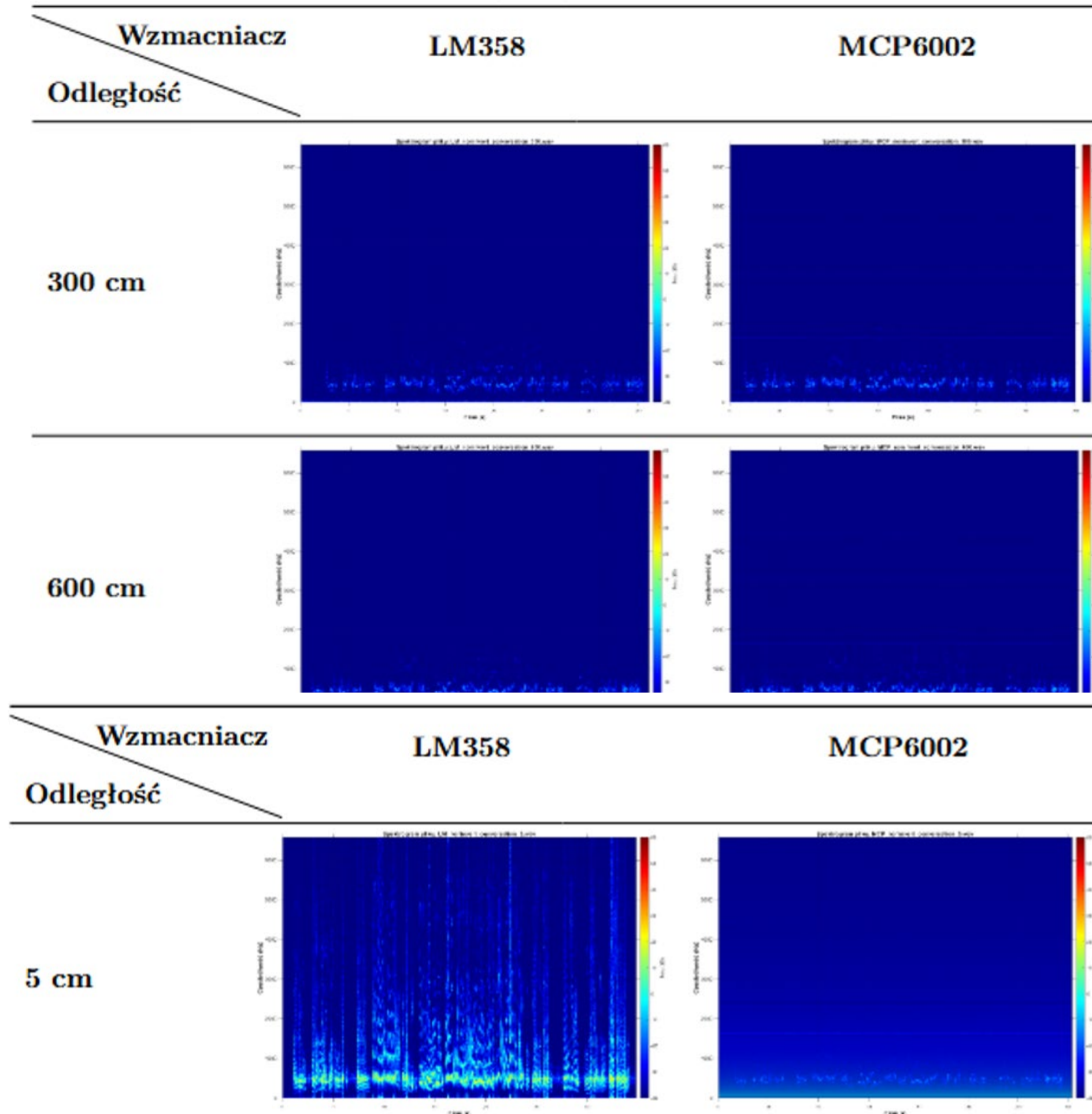
Odwrócenie fizycznej roli przetwornika elektrodynamicznego bez wiedzy użytkownika

Projekt hardware - prototyp:

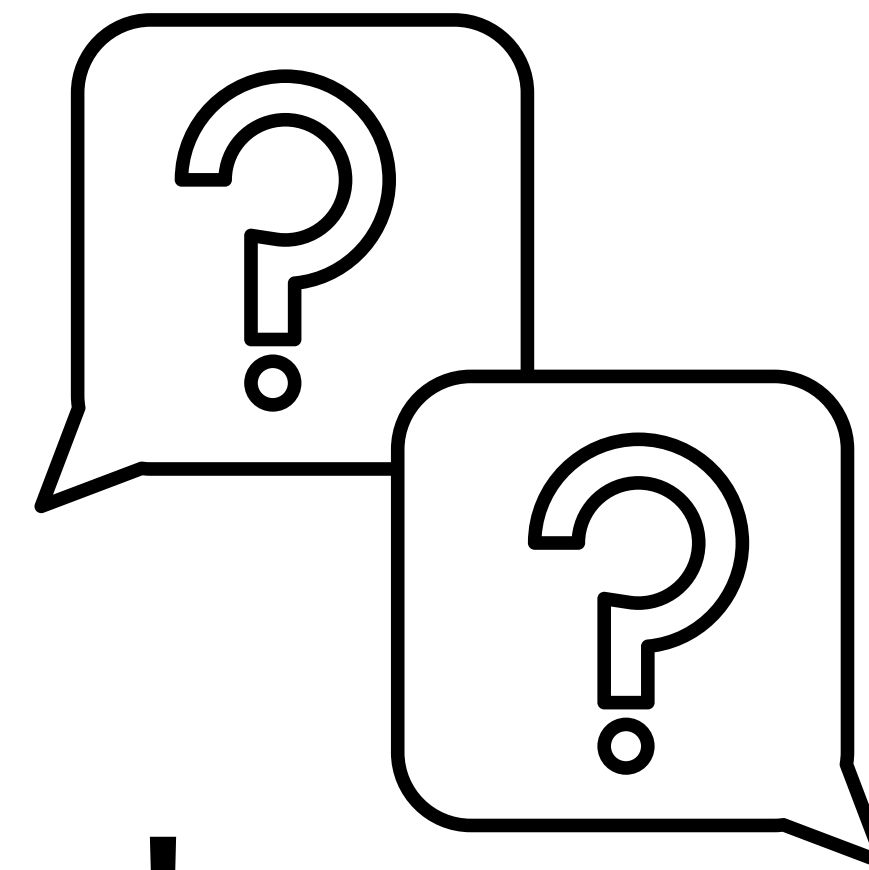
- Konfiguracja odwracająca vs. nieodwracająca sygnał
- Wzmacniacze: LM358 (starszy, ogólny) vs. MCP6002 (nowoczesny audio)
- Testy 3 różnych przetworników
- Arduino UNO + komputer



- Mały okrągły głośnik z silnym magnesem + układ nieodwracający na LM358 umożliwił czytelny odczyt mowy z odległości 6 metrów!
- Starszy wzmacniacz LM358 wykazuje znacznie wyższą podatność na retasking audio i mniejsze zniekształcenia niż nowszy MCP6002
- Rzutniki, smart-głośniki i monitory bez mikrofonu mogą posłużyć jako podsłuch



Wektor ataku	Sprzęt / Budżet	Wynik / Zasięg	Wektor zagrożenia dla IT
Bioakustyczny	Makieta + BT (DIY)	SUKCES (6m)	Ukryte implanty IoT w otoczeniu
Optyczny	Smartfon (240 FPS)	Ograniczenie hardware	Kamery >1000 FPS / Laserów
Elektrodynamiczny	Autorskie PCB + LM358 lub MCP6002	SUKCES (6m)	Rzutniki, smart-głośniki i monitory bez mikrofonu mogą posłużyć jako podsłuch



Dziękuję za uwagę!

