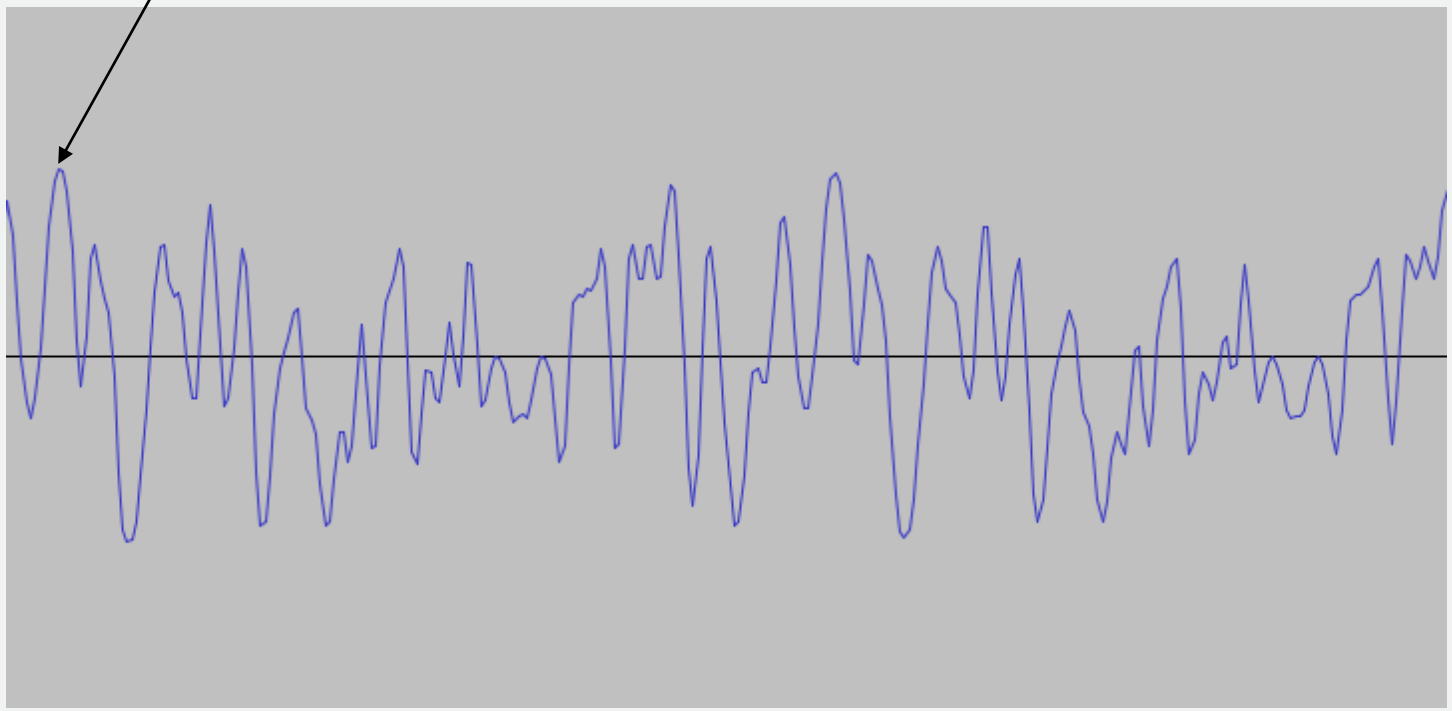
Steganography

Project of Group 3

Introduction

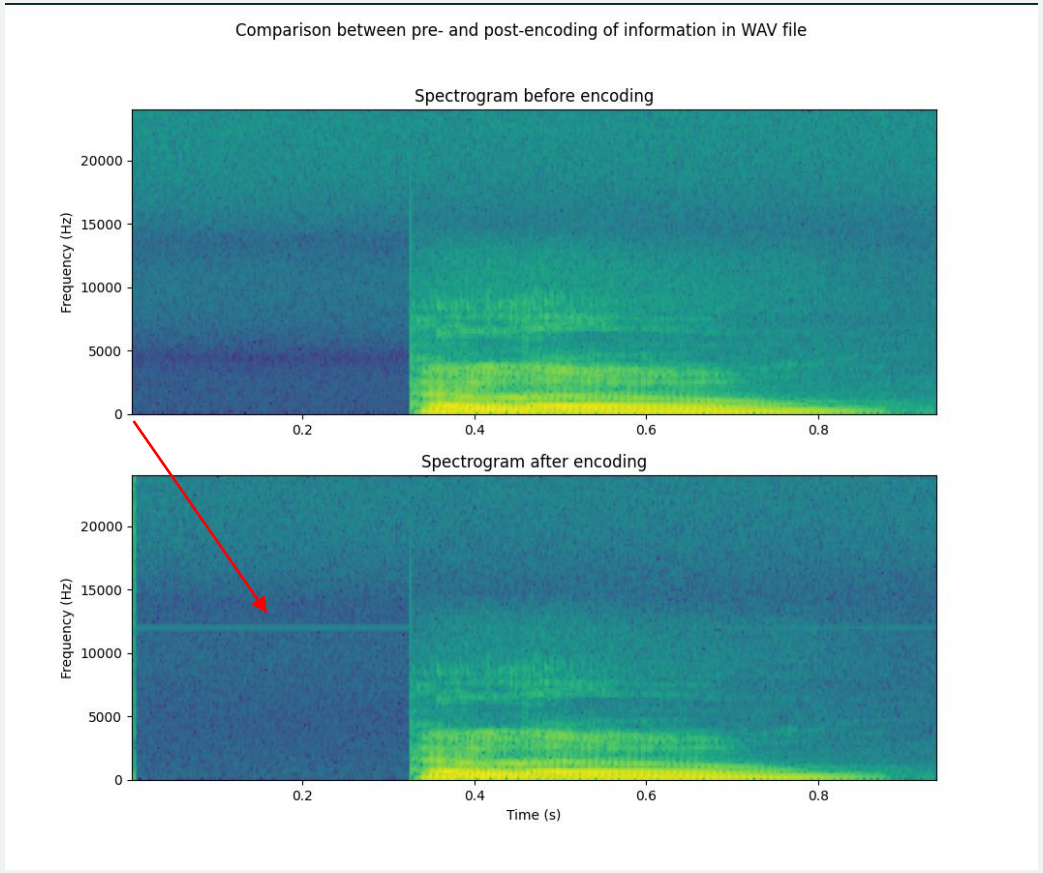
21034 = 0101 0010 0010 1010 = 0101 0010 0010 10**01**



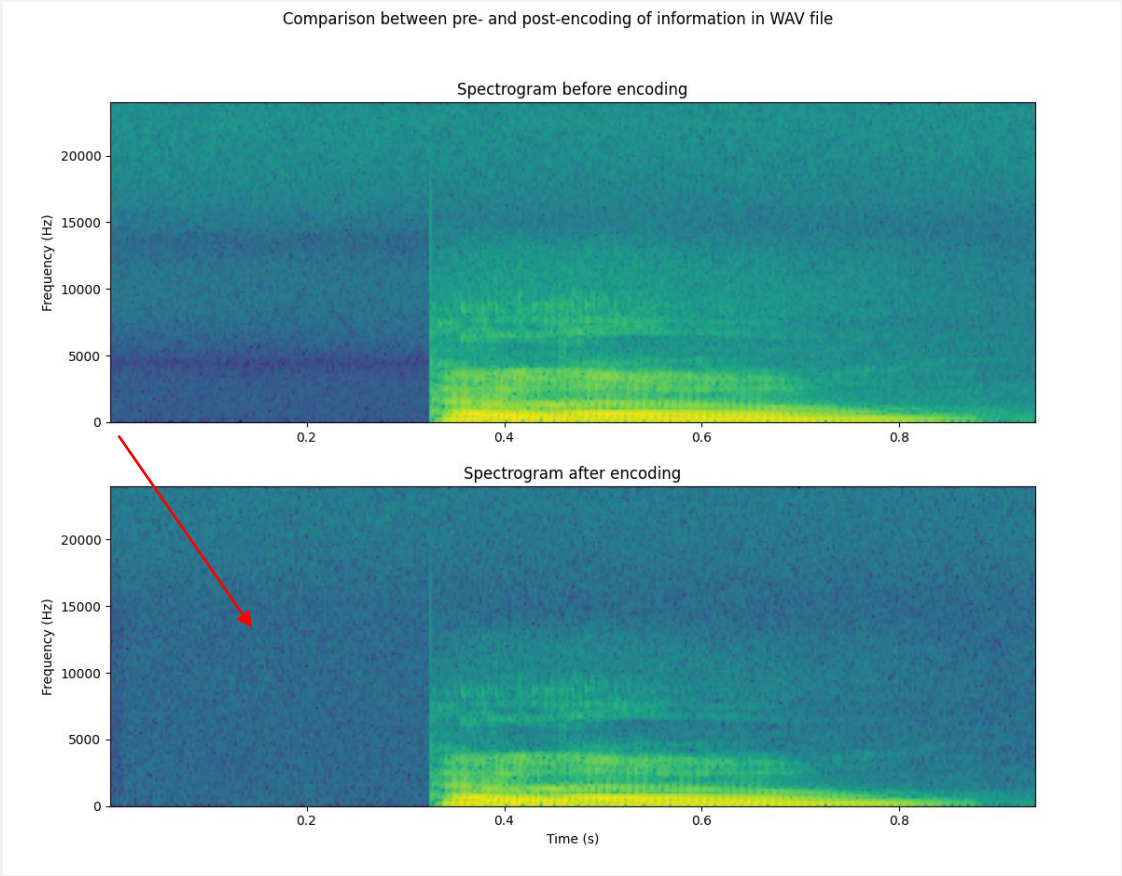
a = 97 = **01** 10 00 01

Audibility

No encryption



AES encryption



Features

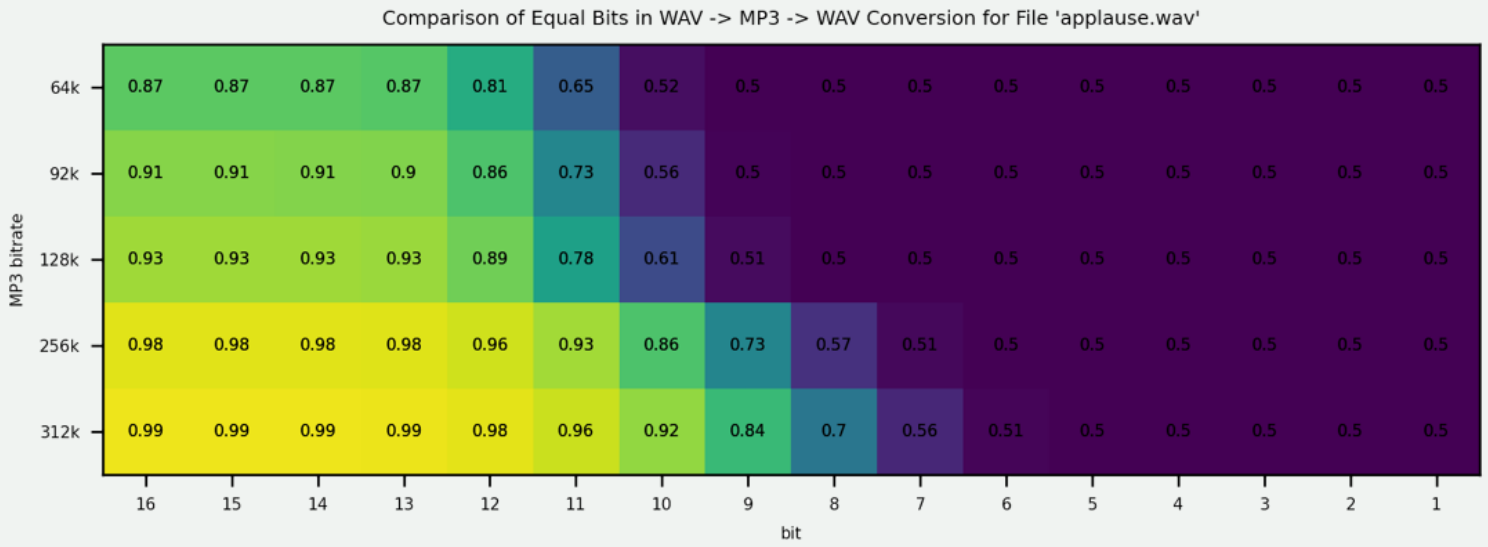
- Small header saved to encode information
- Encryption of data
- Error correction
- Variable number of least significant bits
- Test setup

Encryption

- Password and certificate based
- Content encryption only
- Available algorithms: AES, RSA and Fernet (library specific)
- Hashing: PBKDF2 and Scrypt

Error Correction

- Hamming and Reed Solomon error correction
- Lossy compression formats: original message could not be recreated
- Analyze bit flips (x-axis equals amplitude):



Test audio files

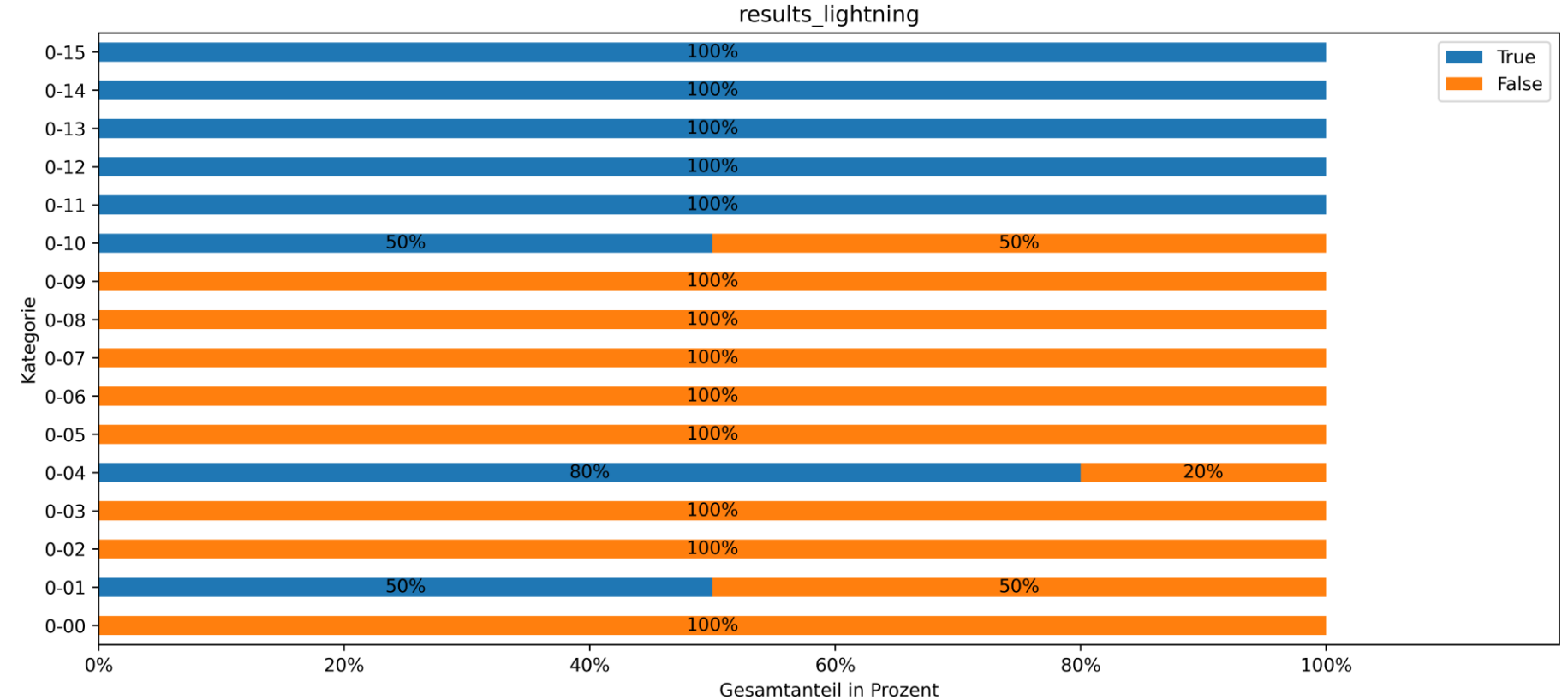
- 1min audio files
- Script to create modified files
- 200kb files encoded
- Every possible number of LSBs

- 4 lsb -> ~10Mbit
- 1 lsb, 254bit error correction -> ~10Kbit

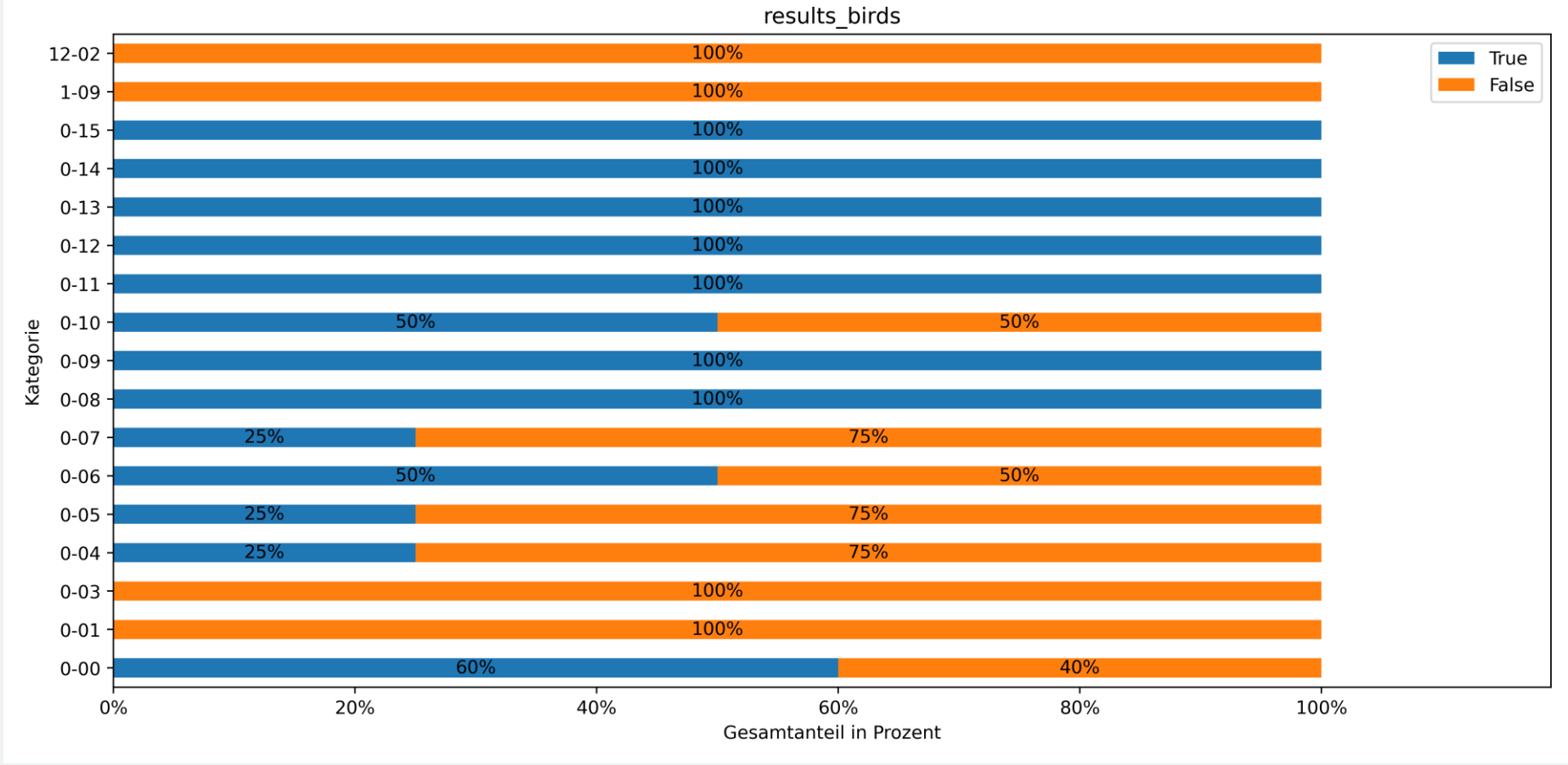
Testsetup A/B Test

- Evaluation of possible encoded message in wav files
- Creation of csv test reports with 15 samples each
- Generation of ~60 test reports
- 90% modified/unmodified files
- 5% unmodified/unmodified files
- 5% modified/modified files

Findings: File Selection



Findings: File Selection

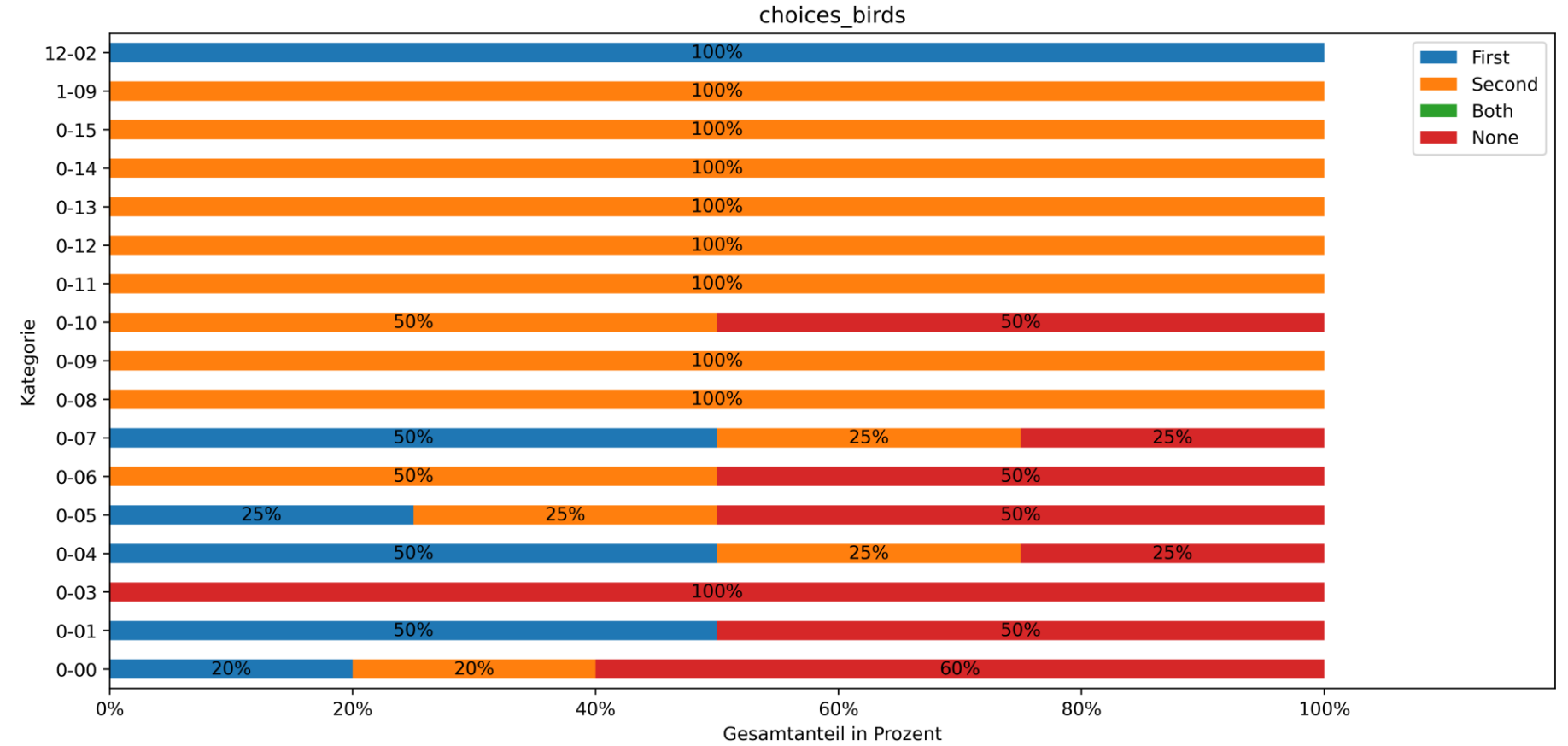


Conclusion

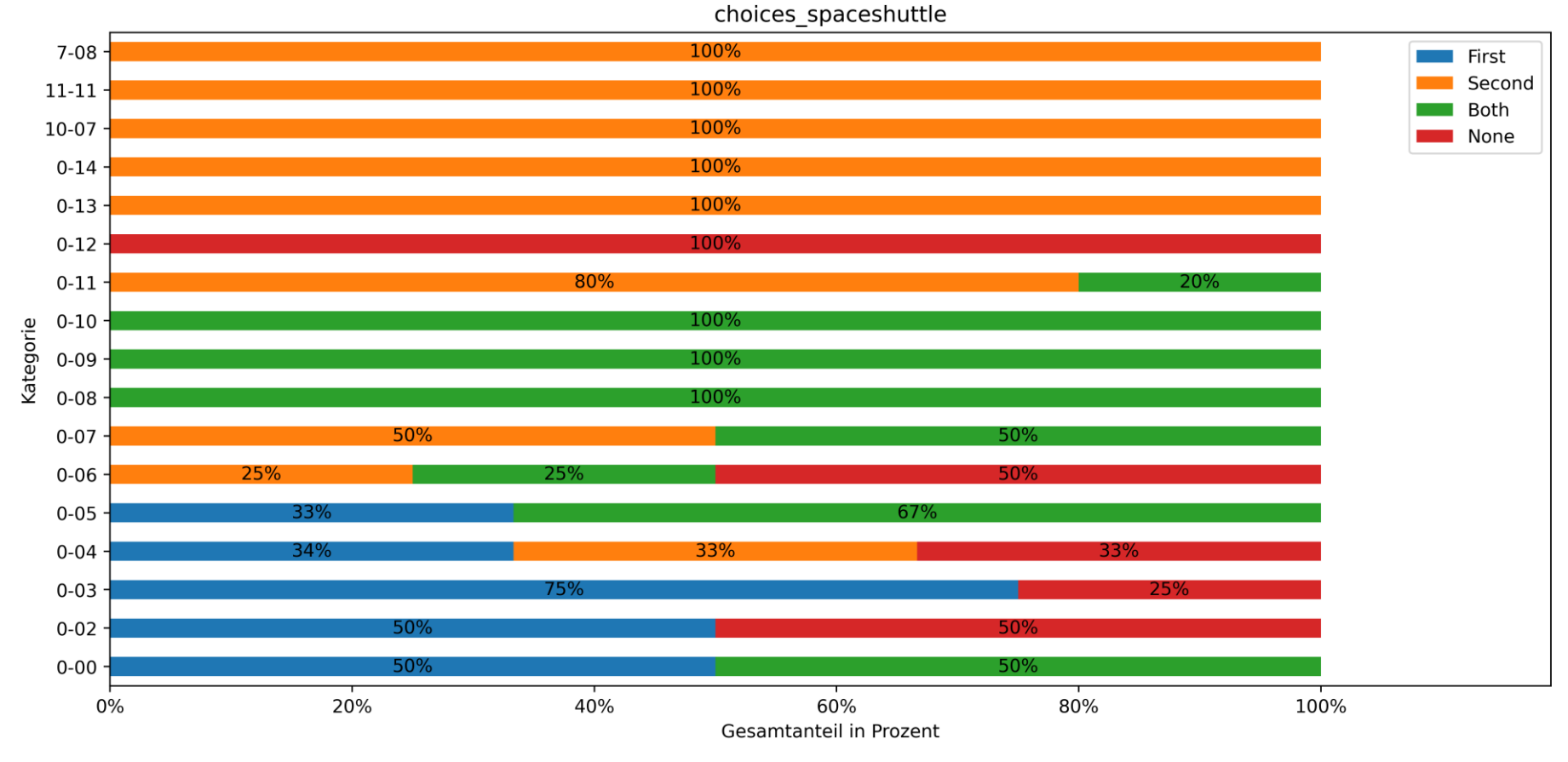
- Decrease risk of manipulation detection by:
  - Smart wav file selection
  - Short message encoding
- Lossy compression format alters message irreversibly

Thank you for your attention!

Findings: User Choices



Findings: User Choices



Findings: User Choices