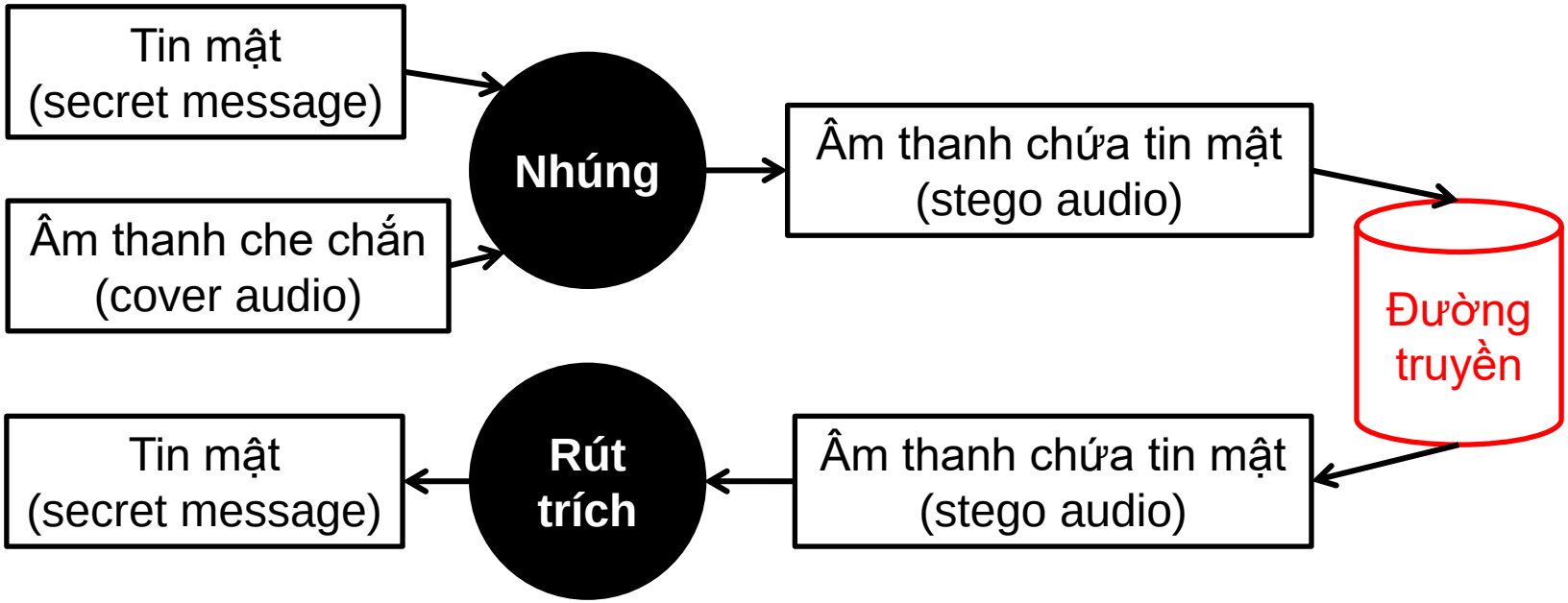
Ẩn tin mật trên âm thanh (Audio steganography)

KHOA CÔNG NGHỆ THÔNG TIN
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

Bài toán ẩn tin mật trên âm thanh

Mong muốn:

- Tính vô hình: người thứ 3 phải khó biết được sự tồn tại của tin mật trong stego audio
- Ngoài ra, còn có các mong muốn khác: sức chứa, tính bền vững

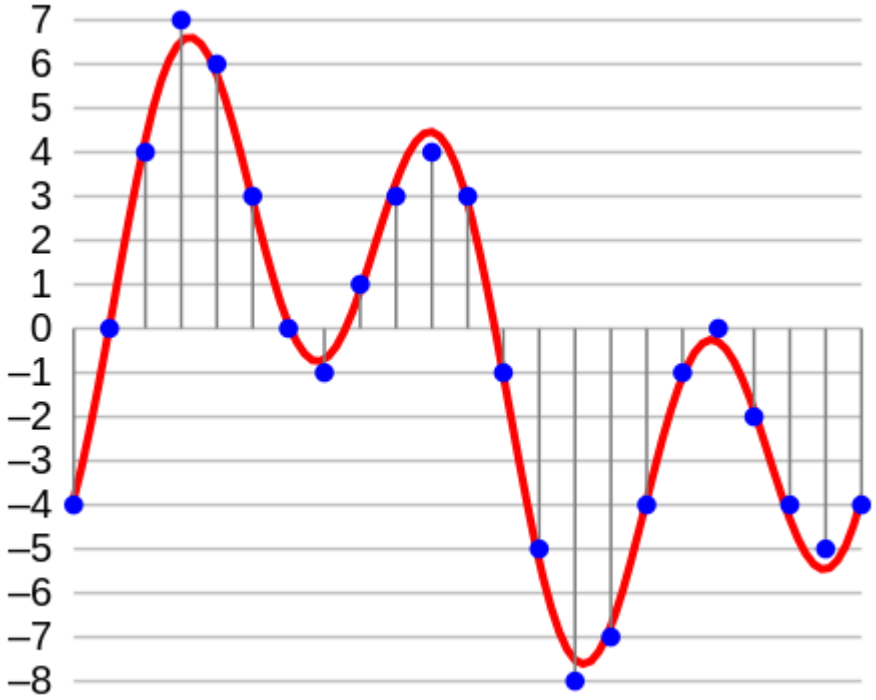


Q: Nên nhúng tin mật vào chỗ nào trong âm thanh?

A: Đầu tiên, cần hiểu về âm thanh ...

Âm thanh được biểu diễn như thế nào trong máy tính?

- Thử đọc một file âm thanh và xem ... (demo)
- Âm thanh được biểu diễn trong máy tính dưới dạng một sóng âm đã được rời rạc hóa.



Đường màu đỏ: sóng nguyên thủy

Các điểm màu xanh: sóng nguyên thủy được rời rạc hóa

- Mỗi điểm được gọi là một **sample**
- Mức độ rời rạc hóa theo chiều y (cường độ) được thể hiện bởi **bit depth** (số bit dùng để lưu giá trị cường độ của một sample)
- Mức độ rời rạc hóa theo chiều x (thời gian) được thể hiện bởi **sample rate** (số sample / s)

Nguồn ảnh: https://en.wikipedia.org/wiki/Audio_bit_depth

Âm thanh được biểu diễn như thế nào trong máy tính?

- File âm thanh có thể **mono** hoặc **stereo**
  - Mono: một sóng
  - Stereo: hai sóng khác nhau (có cùng chiều dài); khi phát ra, một sóng phát ở loa trái, một sóng phát ở loa phải → cho cảm giác thực hơn
- File âm thanh có thể **lossless** hoặc **lossy**
  - Lossy: đọc dữ liệu từ file, chỉnh sửa dữ liệu, ghi dữ liệu đã chỉnh sửa xuống file, đọc dữ liệu lên lại thì dữ liệu đọc được sẽ không giống so với dữ liệu đã ghi trước đó; ví dụ: file *.mp3
  - Lossless: ví dụ, file *.wav

Ẩn dữ liệu ở đâu trên âm thanh? (đang xét file lossless như *.wav)

- Cách đơn giản là ẩn vào các bit LSB của mỗi sample
- Demo ...

Ẩn dữ liệu ở đâu trên âm thanh?

Một cách khác là sử dụng **echo (tiếng vang)**

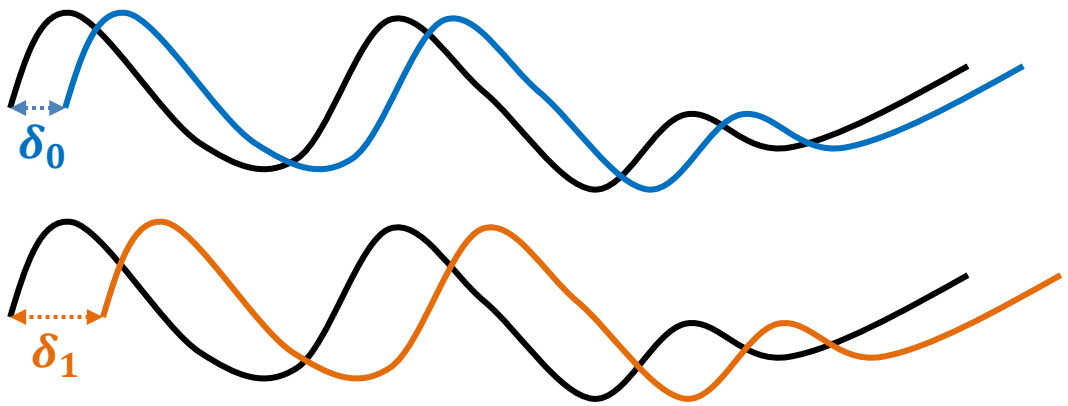
- Echo là gì?
- Dùng echo để nhúng bit mật như thế nào?
- Rút trích như thế nào?

Echo là gì?

- Xem video
- Demo tạo ra một đoạn âm thanh có echo

Dùng echo để nhúng bit mật như thế nào?

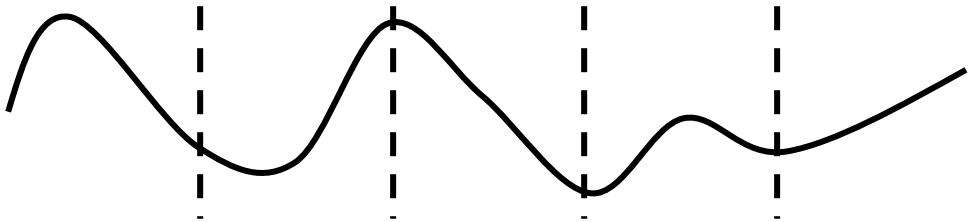
- Để nhúng bit 0: thêm vào cover audio một echo với độ trễ δ_0
- Để nhúng bit 1: thêm vào cover audio một echo với độ trễ δ_1
- Với δ_0 và δ_1 đủ nhỏ, tai người sẽ không nhận biết được echo.



- Vậy là chỉ nhúng được một bit?
- Làm sao để nhúng được nhiều bit?

Dùng echo để nhúng bit mật như thế nào?

Để nhúng nhiều bit, ta chia cover audio ra thành nhiều đoạn và nhúng một bit vào mỗi đoạn bằng cách thêm vào đoạn đó echo có độ trễ δ_0 hoặc δ_1

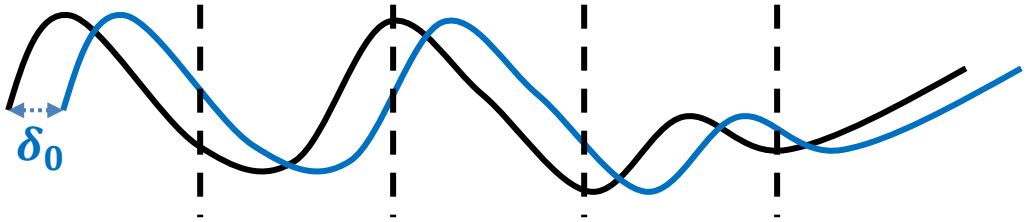


Dùng echo để nhúng bit mật như thế nào?

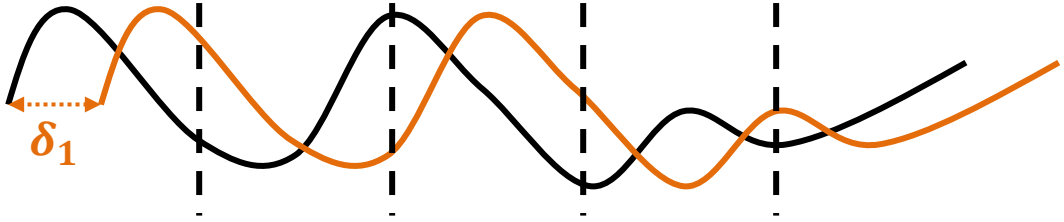
Cụ thể hơn về quá trình nhúng:

- Bước 1: tạo ra 2 cover audio, một có echo ứng với bit 0, một có echo ứng với bit 1

cover audio + echo0



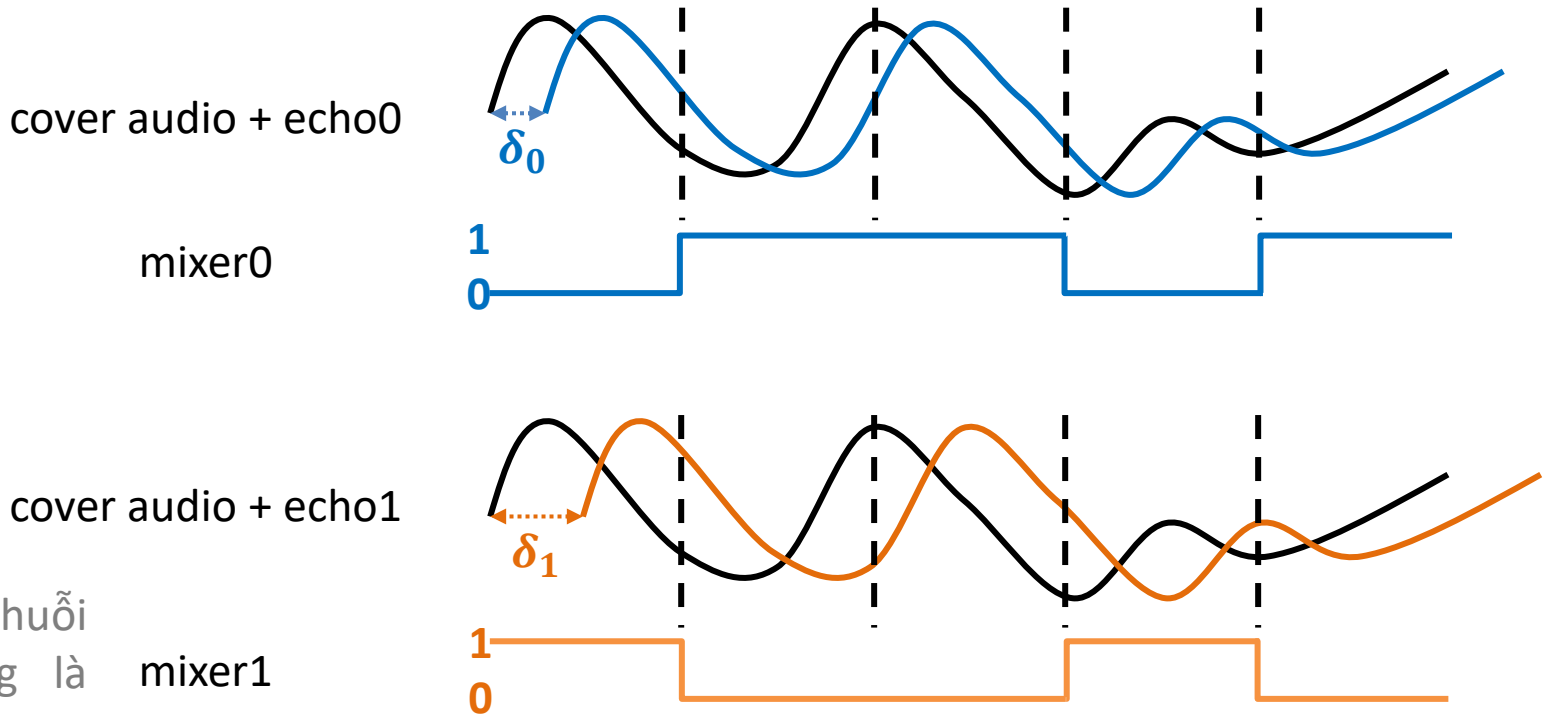
cover audio + echo1



Dùng echo để nhúng bit mật như thế nào?

Cụ thể hơn về quá trình nhúng:

- Bước 2: tạo ra 2 bộ trộn mixer0 và mixer1; mixer1 được tạo ra dựa vào chuỗi bit nhúng, mixer0 = 1 – mixer1

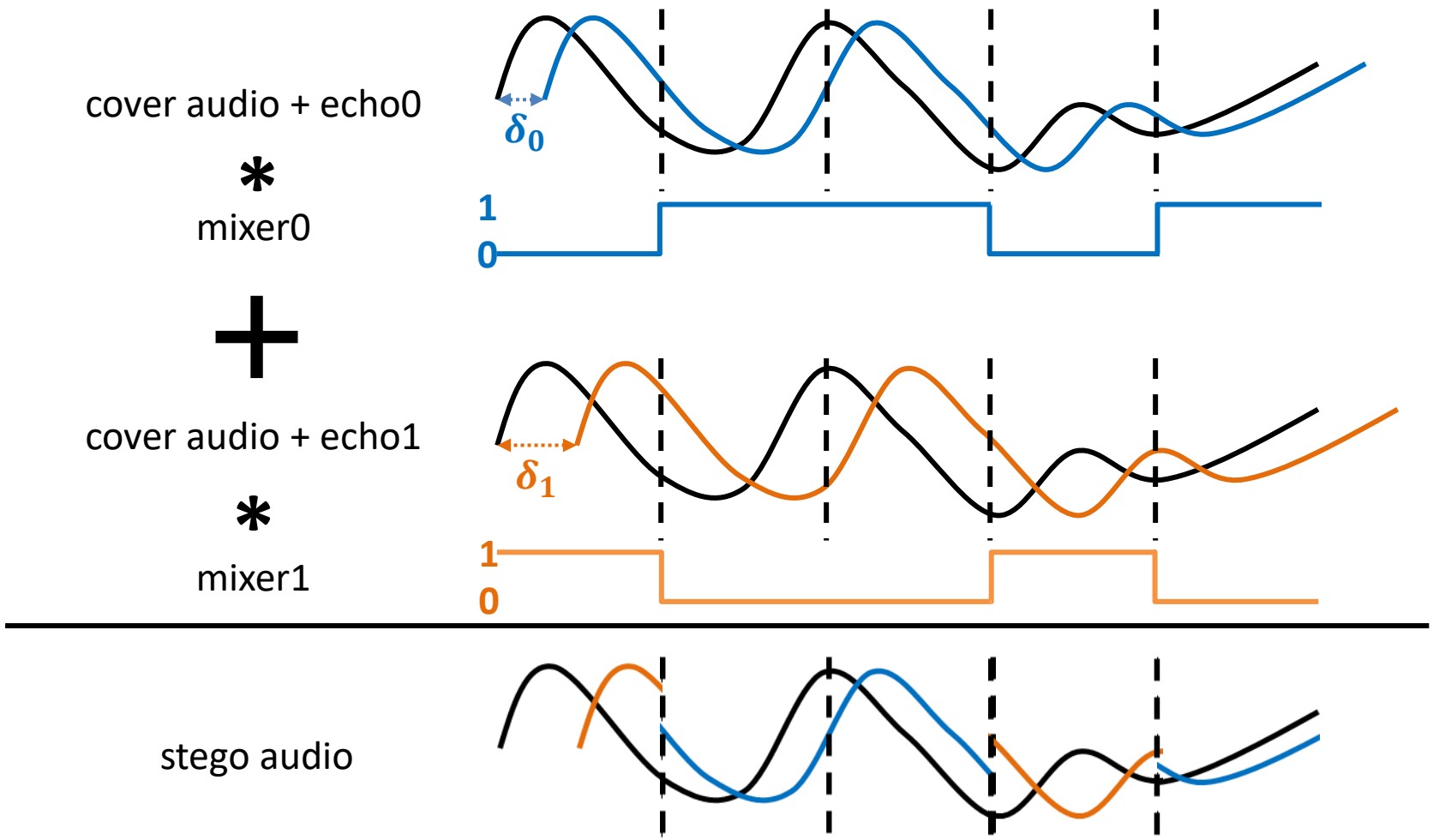


Giả sử chuỗi bit nhúng là 10010

Dùng echo để nhúng bit mật như thế nào?

Cụ thể hơn về quá trình nhúng:

- Bước 3: stego audio = (cover audio + echo0) * mixer0
  + (cover audio + echo1) * mixer1



Input và output của quá trình nhúng

- Input
  - message bits
  - cover audio
  - delta0, delta1
  - decay rate $\in [0, 1]$: tỉ lệ scale cường độ của echo so với sóng âm gốc
    - Cho decay rate nhỏ thì được gì và mất gì?
- Output
  - stego audio

Rút trích như thế nào?

- Để rút trích được, cần biết khi nhúng đã chia ra bao nhiêu đoạn âm thanh
  - Làm sao để Bob và Alice có thể trao đổi thông tin này?
  - Một cách là Alice và Bob có thể gặp nhau một lần và thống nhất chiều dài tối đa của chuỗi bit mật → khi nhúng luôn chia thành chiều dài tối đa của chuỗi bit mật + 1 đoạn âm thanh, thêm 100... vào chuỗi bit mật và nhúng trên tất cả các đoạn âm thanh

Rút trích như thế nào?

- Với một đoạn âm thanh của stego audio, cần xác định xem có echo ở độ trễ nào
- Giả sử xác định được có echo ở độ trễ 0.5 s → bit 0 hay bit 1?
- Để biết là bit 0 hay 1, ta hãy xem thêm độ trễ của echo ở các đoạn âm thanh khác
  - → sẽ có tất cả 2 giá trị độ trễ δ_0 (bit 0) và δ_1 (bit 1), nhưng không biết đâu là δ_0, đâu là δ_1
  - → Alice và Bob có thể thống nhất với nhau là $\delta_0 < \delta_1$

Rút trích như thế nào?

- Với một đoạn âm thanh của stego audio, làm sao để xác định được độ trễ của echo?
- Một cách là tính autocorrelation
  - Xem demo