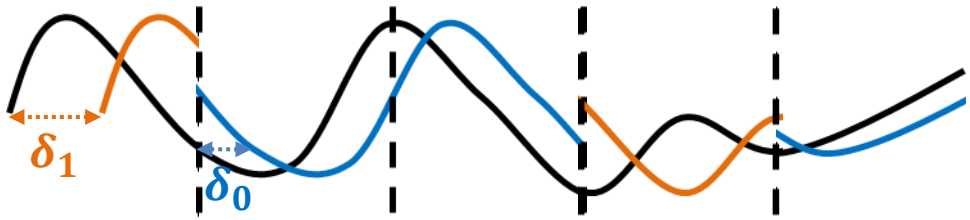
Watermarking

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

Buổi trước: ẩn tin mật trên âm thanh bằng phương pháp echo

Nhúng

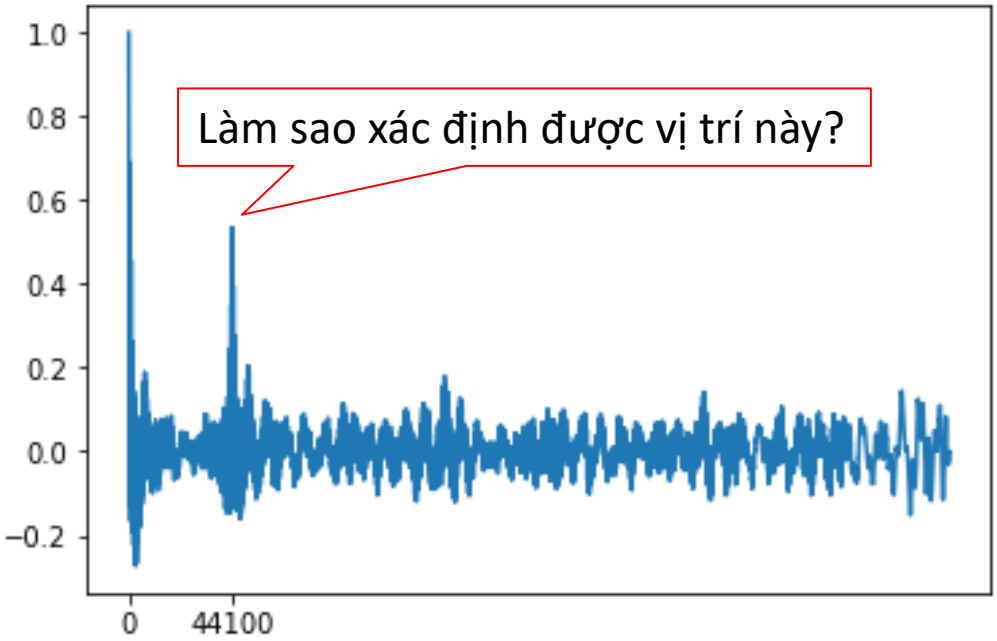


Buổi trước: ẩn tin mật trên âm thanh bằng phương pháp echo

Rút trích

Input: stego audio, num segments (số đoạn âm thanh được chia ra khi nhúng)

- Bài toán đặt ra là: với một đoạn âm thanh (một segment) trong stego audio, làm sao để xác định được độ trễ của echo?
- Một cách là tính autocorrelation tại các độ trễ khác nhau...



Buổi trước: ẩn tin mật trên âm thanh bằng phương pháp echo

Rút trích

Input: stego audio, num segments (số đoạn âm thanh được chia ra khi nhúng), delta0 (δ_0), delta1 (δ_1)

- Bài toán đặt ra là: với một đoạn âm thanh (một segment) trong stego audio, cần xác định có echo ở độ trễ δ_0 hay δ_1?
- Cho luôn δ_0 và δ_1 thì có thực tế không?
  - Có thể được, vì một δ_0 và một δ_1 có thể dùng cho nhiều cover audio khác nhau
- Một cách giải đơn giản cho bài toán này là so sánh giá trị autocorrelation tại 2 độ trễ δ_0 và δ_1, ở đâu có giá trị autocorrelation lớn hơn thì ở đó có echo

Nội dung môn học

- Ẩn dữ liệu (data/information hiding)
  - Steganography ✓
  - Watermarking ← Buổi này
- Chia sẻ thông tin mật (secret sharing)

Vấn đề 1

Giả sử bạn chụp được một bức ảnh đẹp và đưa lên mạng. Những người khác sẽ có thể dễ dàng sao chép ảnh của bạn, thậm chí có thể nói ảnh là của họ, và sử dụng cho lợi ích của cá nhân họ. Làm sao để hạn chế vấn đề này?

Một giải pháp

Nhúng thông tin của chủ sở hữu vào bức ảnh trước khi đưa lên mạng.

Nguồn ảnh: http://www.aoaophoto.com/watermark-images.htm

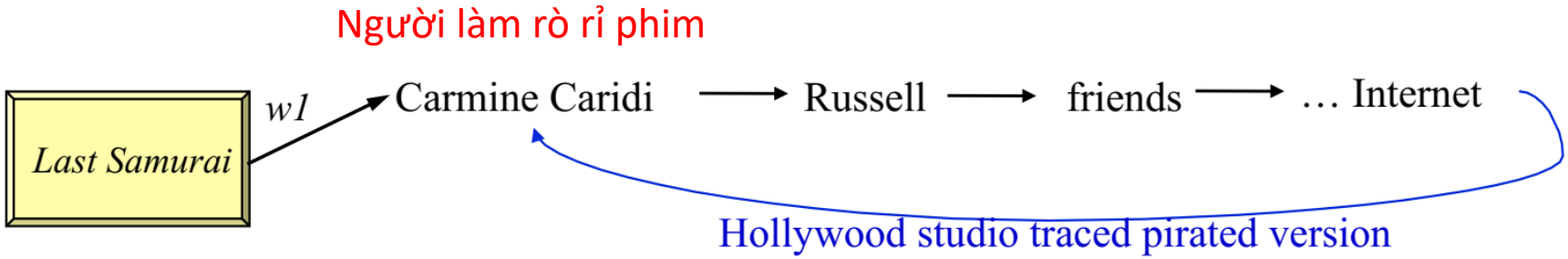
Vấn đề 2

Giả sử bạn là nhà xuất bản sách điện tử, bạn bán nhiều bản sao của một file sách cho nhiều khách hàng. Một khách hàng có thể tự ý tạo ra các bản sao, gửi cho người này người kia; cuối cùng, kết quả là file sách xuất hiện trên mạng và mọi người có thể tự do down. Làm sao để hạn chế vấn đề này?

Một giải pháp

Khi bán ra một bản sao cho một khách hàng, nhúng vào đó một mã dành riêng cho khách hàng đó. Nếu file sách bị rò rỉ trên mạng, nhà xuất bản có thể rút trích ra mã để biết được nguồn rò rỉ là từ khách hàng nào.

Ví dụ thực tế



Nguồn ảnh: http://www.cs.ucsb.edu/~htzheng/teach/cs182/schedule/pdf/lecture14.pdf

Watermark là gì?

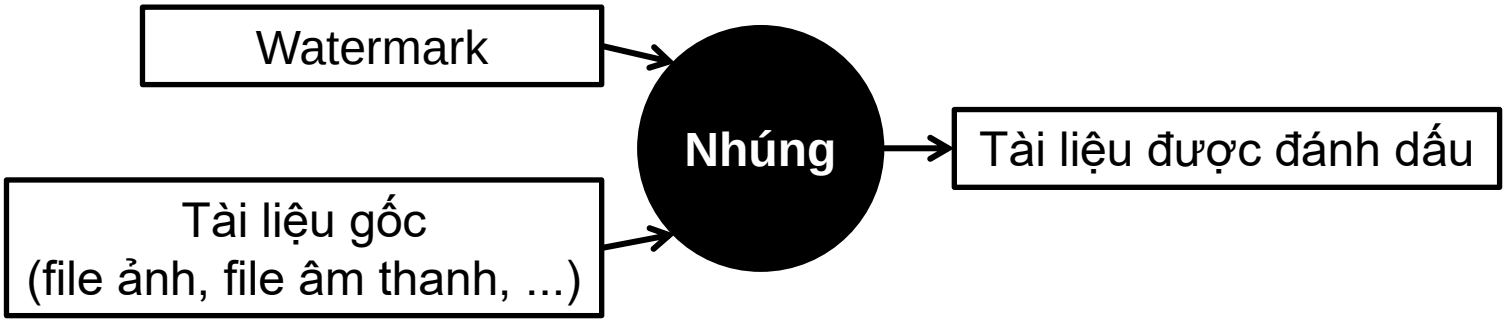
Watermark (digital watermark) là một "dấu" (mark) được nhúng vào một file dữ liệu (văn bản, hình ảnh, âm thanh, ...) nhằm nói lên thông tin nào đó về file dữ liệu (vd, thông tin về chủ sở hữu của file dữ liệu, hay thông tin về khách hàng mua file dữ liệu)

Watermarking khác gì với steganography?

Quá trình nhúng watermark

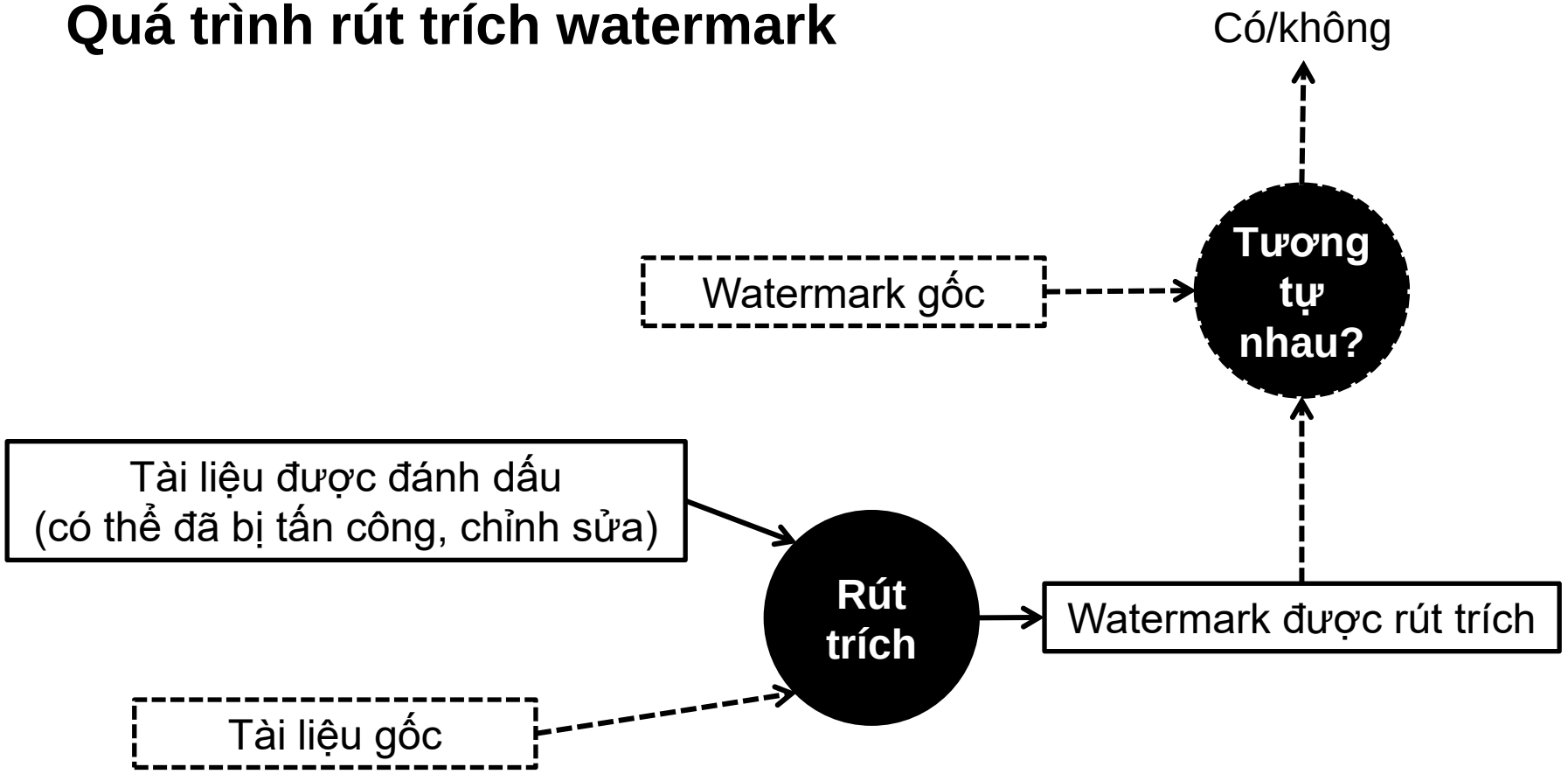
Trong 3 tiêu chí vô hình – bền vững – sức chứa:

- steganography đặt nặng vào tiêu chí vô hình và sức chứa
- watermarking đặt nặng vào tiêu chí bền vững và vô hình



Watermarking khác gì với steganography?

Quá trình rút trích watermark



Các phần gạch đứt là có thể có thêm

Có thể dùng các thuật toán của steganography cho watermarking không?

Có thể dùng được nếu thuật toán steganography có tính bền vững cao (bên cạnh tính vô hình cao)

Quizz: copyright

Xem và làm trên moodle (ở phía dưới, chỗ buổi 10)

Watermarking trên ảnh (hoặc âm thanh) bằng phương pháp Cox [1]

Ý tưởng

- Dùng watermark là một véc-tơ gồm nhiều phần tử, mỗi phần tử có giá trị ngẫu nhiên và có độ lớn nhỏ (xem watermark là một id ứng với một người nào đó)
- Nhúng watermark gồm n phần tử vào n hệ số quan trọng trong không gian tần số
- Khi chứng thực, rút trích ra watermark w^* từ ảnh (có thể đã bị chỉnh sửa) và tính độ tương quan với watermark gốc w, nếu độ tương quan lớn hơn ngưỡng t → ảnh có w

[1] Cox et al., Secure Spread Spectrum Watermarking for Multimedia, 1997, Cited by 8248

Watermarking trên ảnh (hoặc âm thanh) bằng phương pháp Cox [1]

Ý tưởng

- Dùng watermark là một véc-tơ gồm nhiều phần tử, mỗi phần tử có giá trị ngẫu nhiên và có độ lớn nhỏ (xem watermark là một id ứng với một người nào

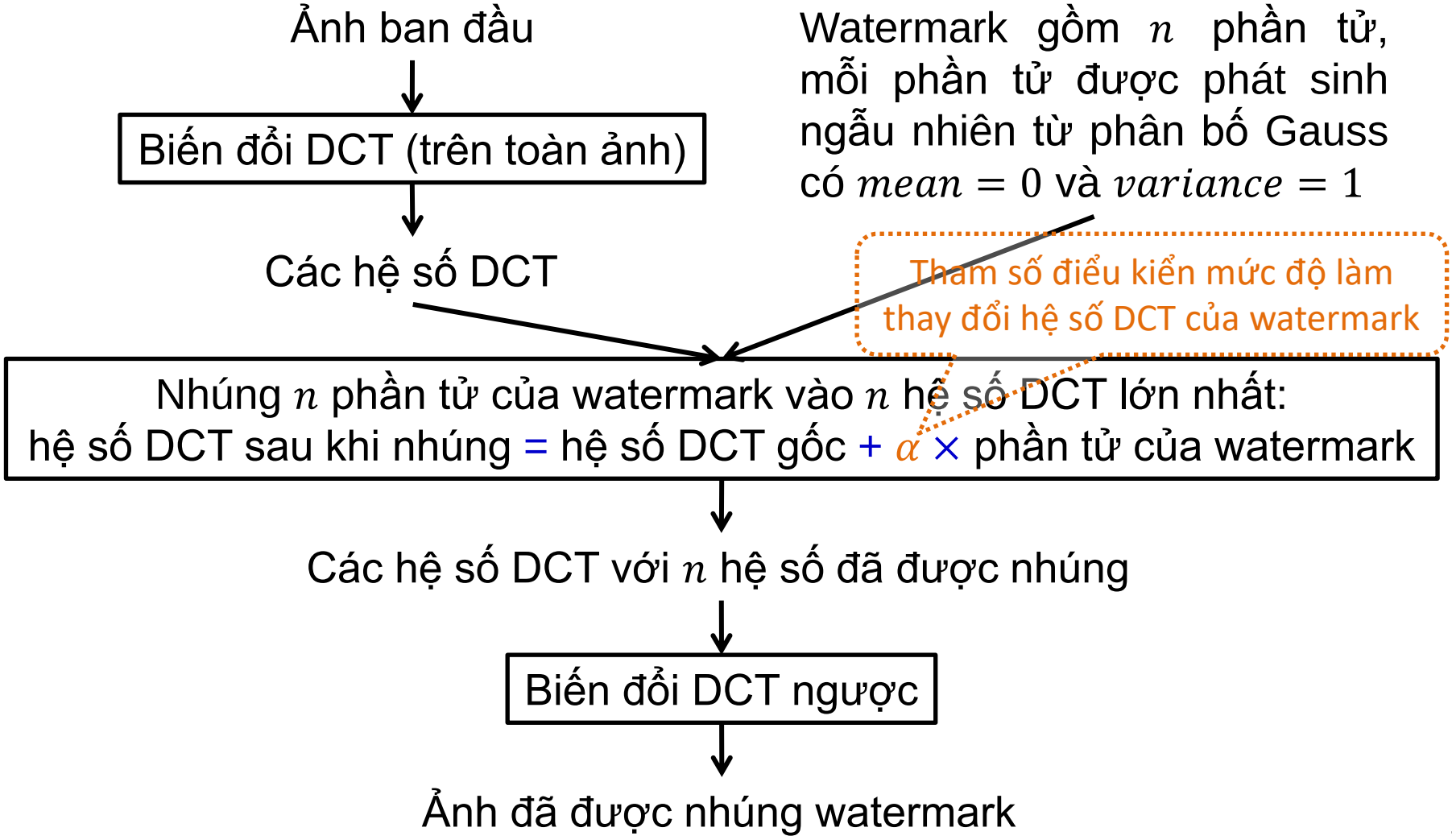
Bền vững là do

Vô hình là do

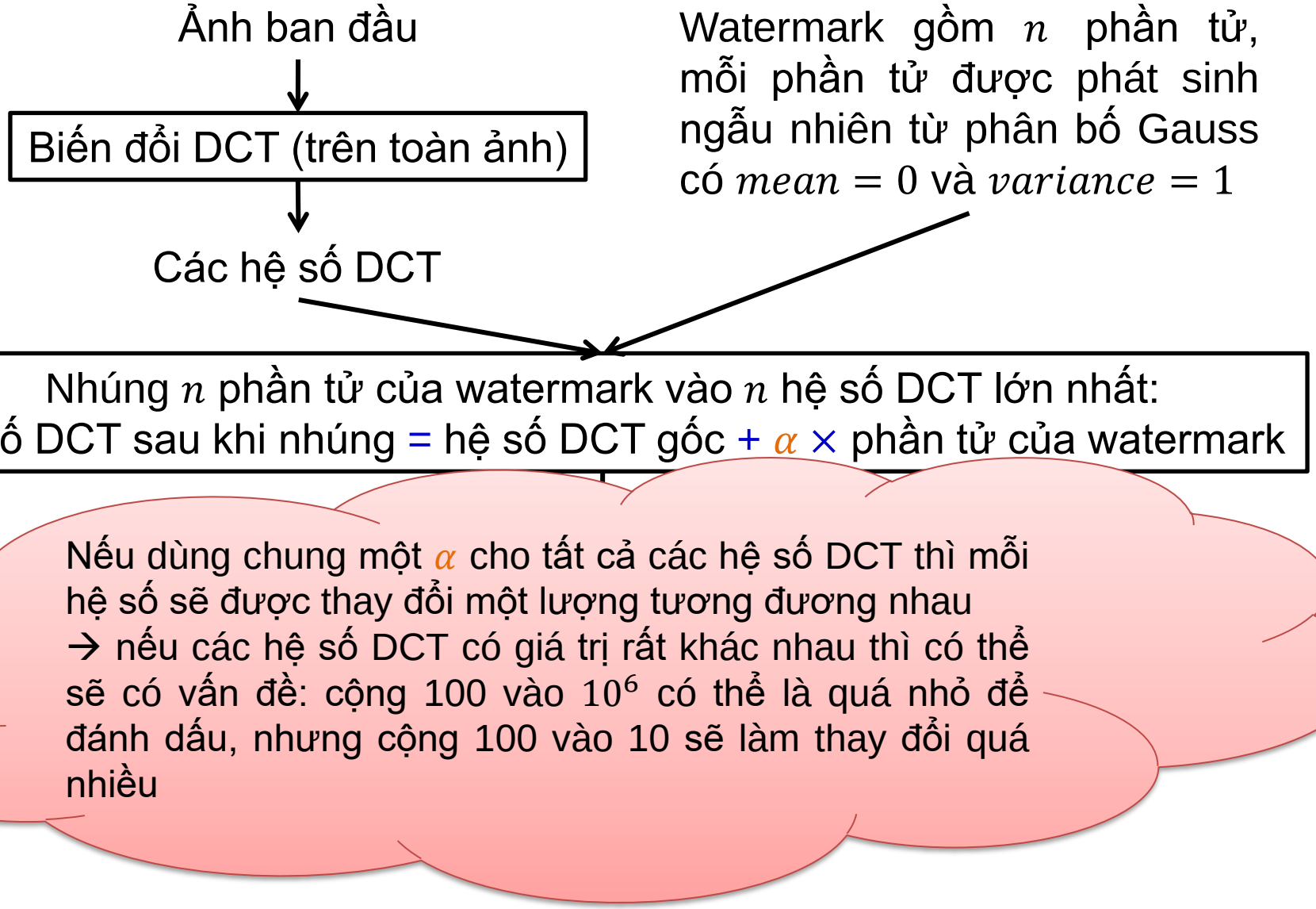
- Nhúng watermark gồm n phần tử vào n hệ số quan trọng trong không gian tần số
- Khi chứng thực, rút trích ra watermark w^* từ ảnh (có thể đã bị chỉnh sửa) và tính độ tương quan với watermark gốc w, nếu độ tương quan lớn hơn ngưỡng t → ảnh có w

[1] Cox et al., Secure Spread Spectrum Watermarking for Multimedia, 1997, Cited by 7925

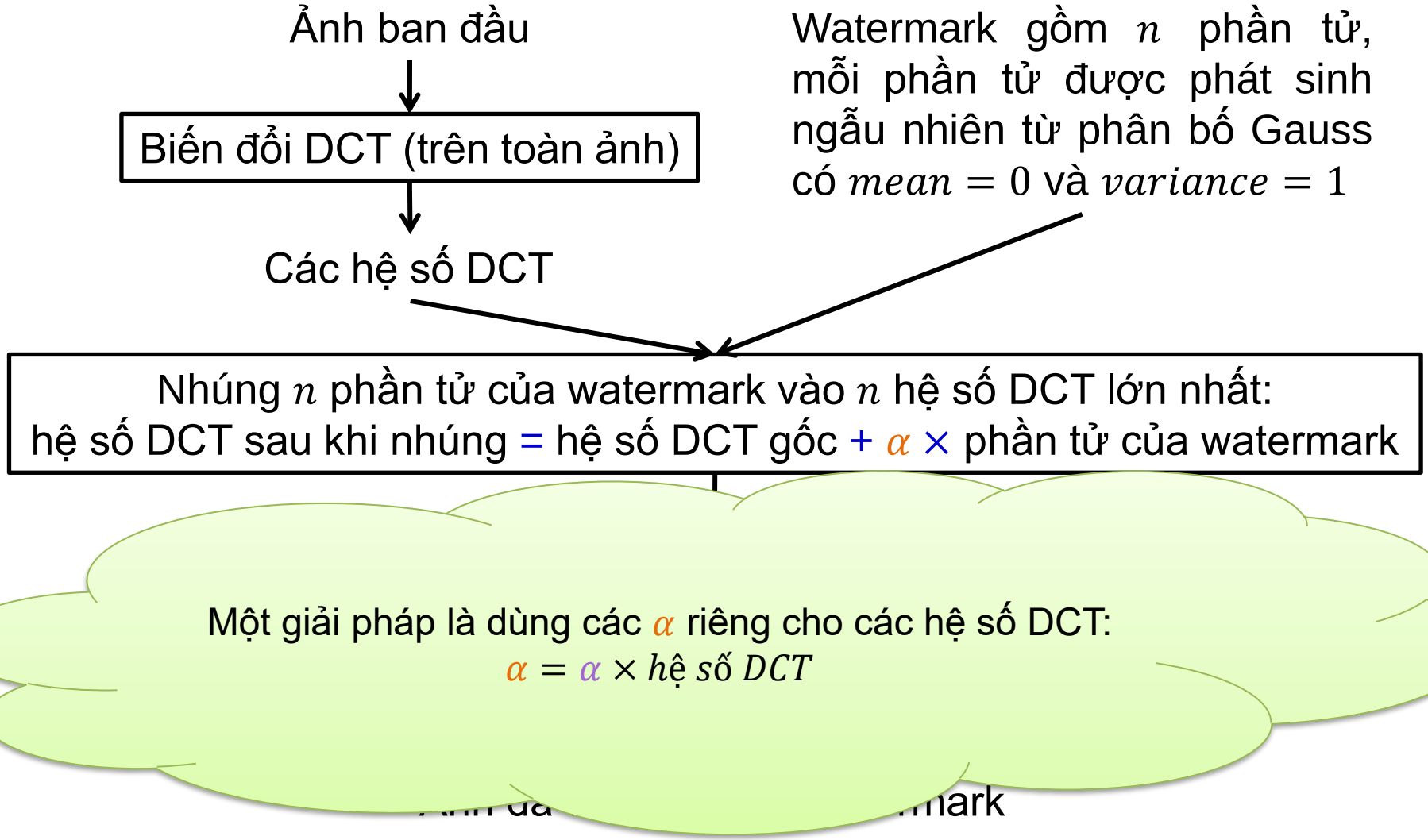
Watermarking trên ảnh bằng phương pháp Cox: quá trình nhúng



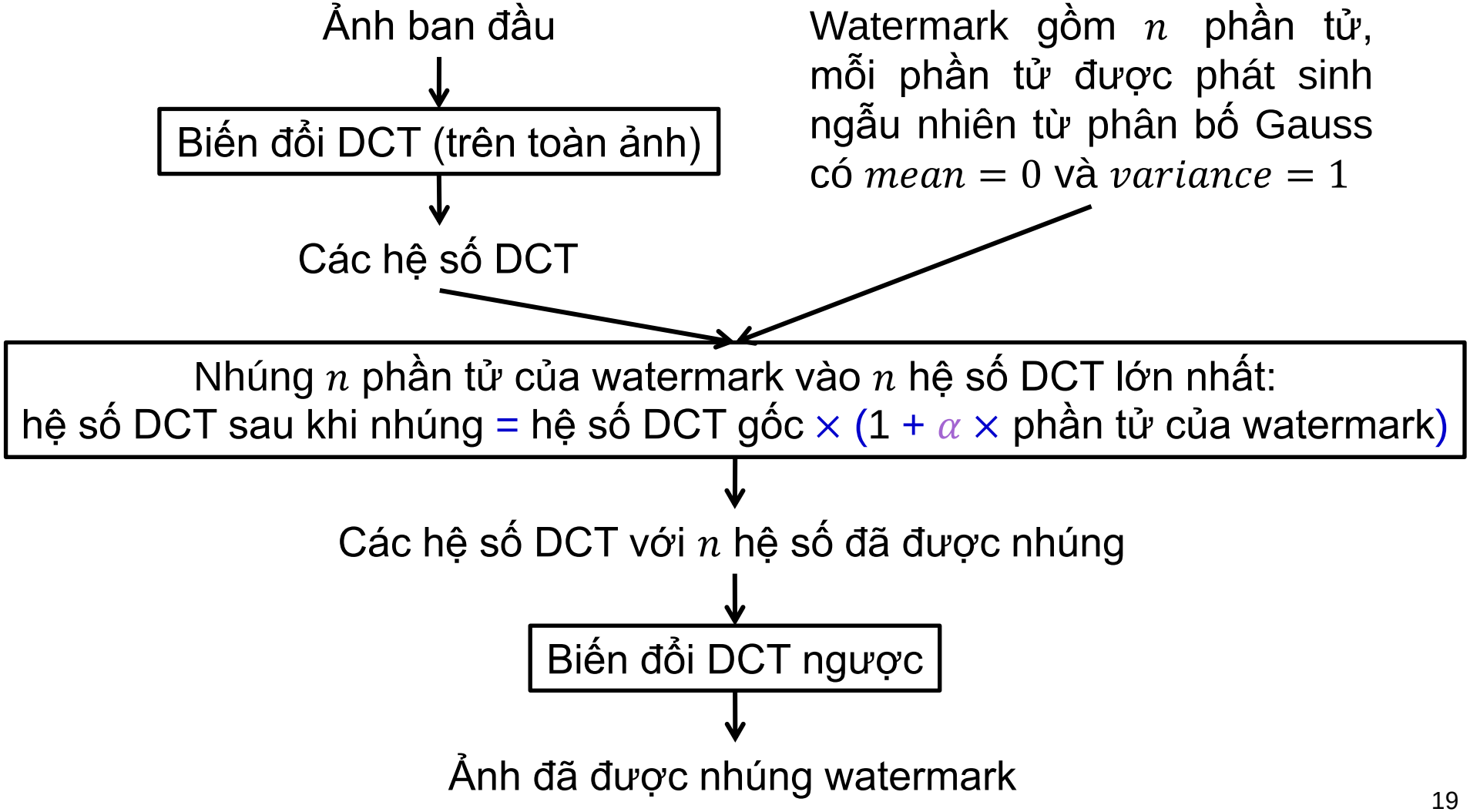
Watermarking trên ảnh bằng phương pháp Cox: quá trình nhúng



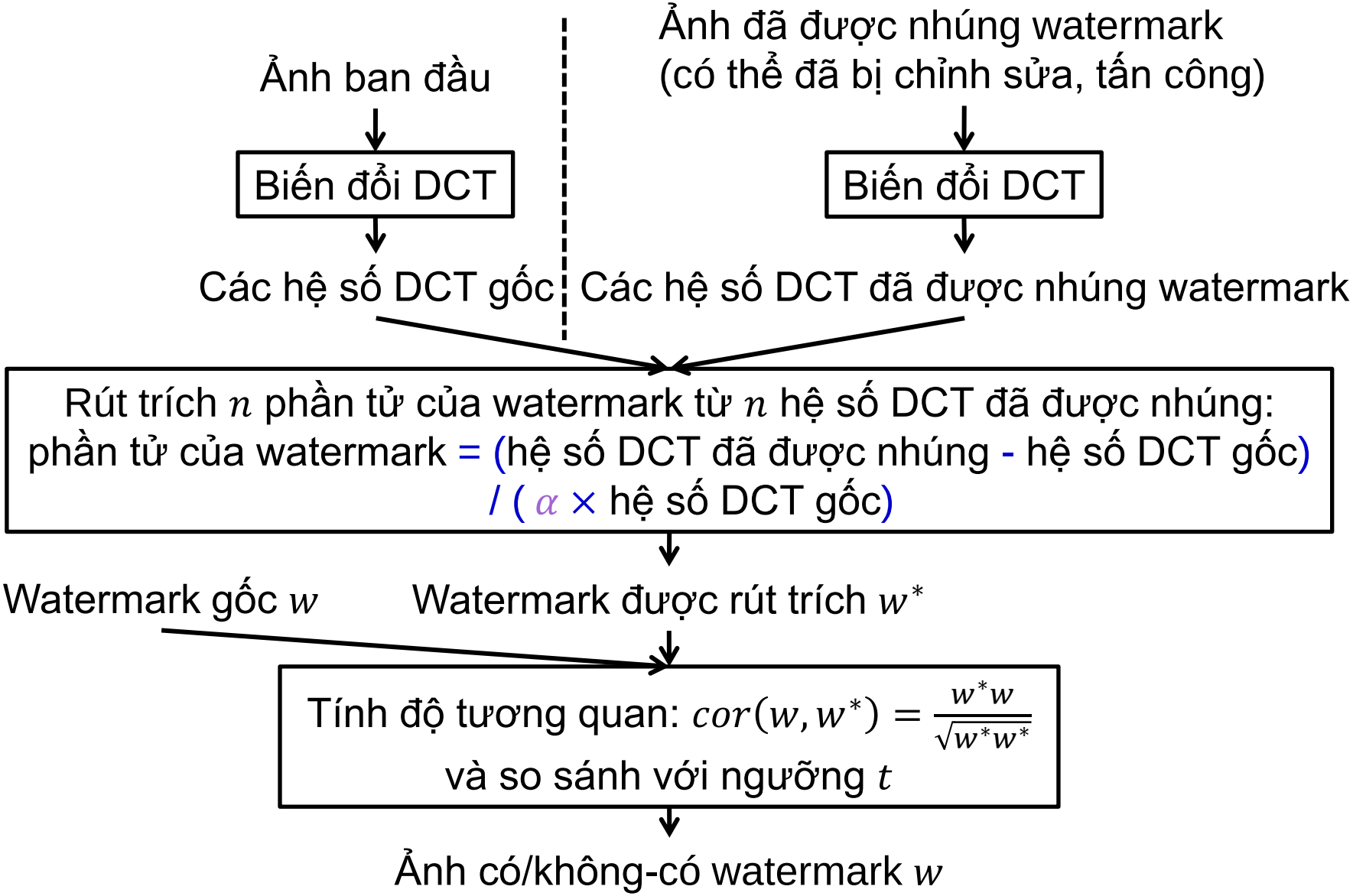
Watermarking trên ảnh bằng phương pháp Cox: quá trình nhúng



Watermarking trên ảnh bằng phương pháp Cox: quá trình nhúng



Watermarking trên ảnh bằng phương pháp Cox: quá trình rút trích



Watermarking trên ảnh bằng phương pháp Cox

Chọn α, chiều dài n của watermark, ngưỡng t bằng bao nhiêu?

- Một cách là tiến hành các thí nghiệm để chọn ra giá trị phù hợp
- Trong bài báo, tác giả chọn:
  - $\alpha = 0.1$
  - $n = 1000$
  - $t = 6$

Demo ...