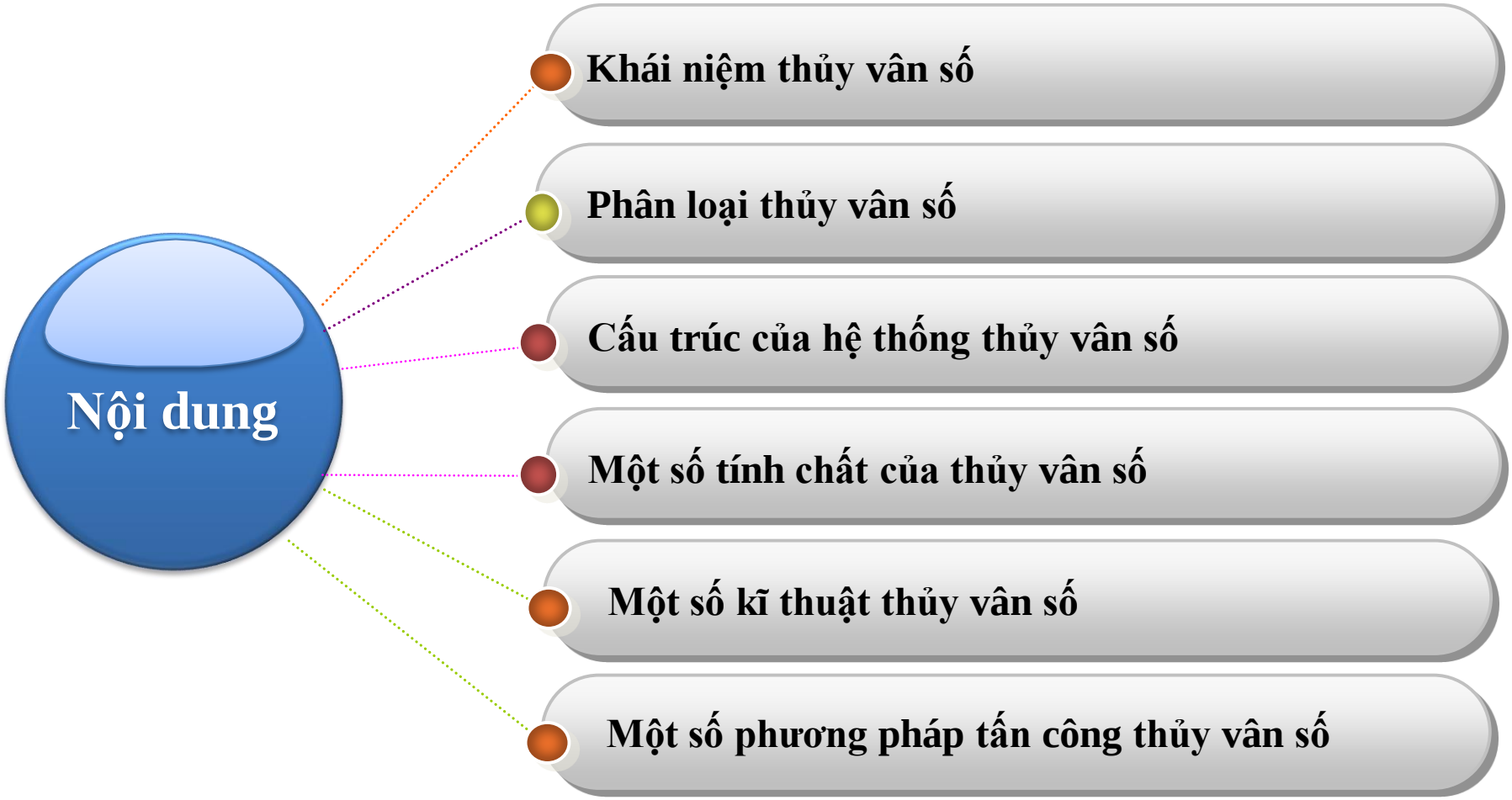
Chương 4. Thủy vân số



Khái niệm thủy vân số

- Lịch sử ra đời
  - Tên gọi *thủy vân*
    - Vẫn còn nhiều tranh cãi
    - Cho rằng thực chất thủy vân không tạo ra từ mà xuất hiện khi nhúng giấy vào nước

Khái niệm thủy vân số (..)

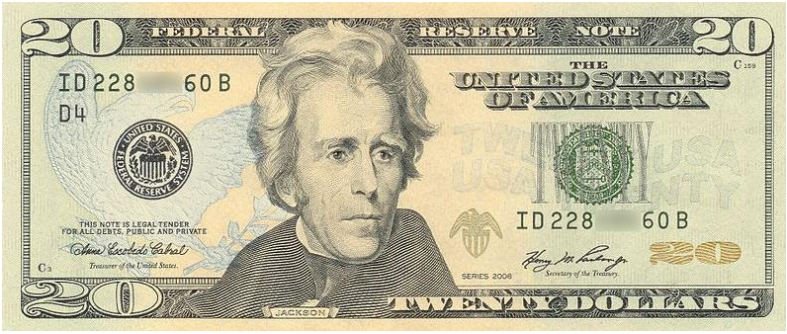
- Lịch sử ra đời (..)
  - Được xem xuất hiện lần đầu tiên trong lĩnh vực sản xuất giấy truyền thống vào năm 1282 tại Italia
    - Là các dấu hiệu hay hình mờ được in chìm trong giấy nhằm xác định nhãn hiệu của những tờ giấy
  - Khoảng thế kỉ XVIII, thủy vân trên giấy được làm ở châu Âu và Mỹ
    - Là những nhãn hiệu ghi lại ngày tháng sản xuất giấy và xác định kích cỡ bản đầu của tờ giấy
    - Chống làm giả tiền và các tư liệu khác

Khái niệm thủy vân số (..)

- Lịch sử ra đời (..)
  - William Congreve (Anh) đã phát minh ra kĩ thuật làm thủy vân màu bằng cách chèn các vật liệu đã được nhuộm màu vào giữa tờ giấy trong quá trình tạo thủy vân
    - Rất khó thực hiện nên ngân hàng của Anh từ chối sử dụng

Khái niệm thủy vân số (..)

- Lịch sử ra đời (..)
  - William Henry Smith (Anh) đã phát minh ra một kĩ thuật thực tế hơn
    - Sử dụng các đường vân điêu khắc mỏng để chèn vào các đường gờ của giấy thay cho các dây đã sử dụng trước đây
    - → Tạo ra thủy vân đẹp hơn với nhiều bóng xám khác nhau
    - Chính là kĩ thuật cơ bản được sử dụng ngày nay đối với khuôn mặt của tổng thống Jackson trên tờ tiền 20$ của Mỹ



Khái niệm thủy vân số (..)

- Lịch sử ra đời (..)
  - Năm 1954, Emil Hembrooke (tập đoàn Muzak) đã sắp xếp một tác phẩm âm nhạc "thủy vân" bằng cách chèn một mã nhận dạng
  - Thủy vân cũng bị làm giả nhiều đặc biệt là thủy vân dùng để bảo vệ tiền giấy
    - Năm 1779, tạp chí Gentleman's đưa tin John Mathison đã phát hiện ra một phương pháp làm giả thủy vân của các giấy tờ ngân hàng

Thúc đẩy sự phát triển các kĩ thuật thủy vân

Khái niệm thủy vân số (..)

- Lịch sử ra đời (..)
  - Rất khó xác định được thuật ngữ *thủy vân số* (Digital watermarking) ra đời từ thời điểm nào
    - Năm 1979, Szepanski đã mô tả một mô hình phát hiện được đặt vào các tài liệu với mục đích chống giả mạo
    - Năm 1988, Holt và các cộng sự đã mô tả một phương pháp nhúng mã nhận dạng vào một tín hiệu số
    - Một số tài liệu cho biết Komatsu và Tominaga đã lần đầu tiên sử dụng thuật ngữ “thủy vân số” vào năm 1988

Khái niệm thủy vân số (..)

- ***Khái niệm***
  - Thủy vân số là quá trình nhúng dữ liệu (hay được gọi là thủy vân) vào một đối tượng đa phương tiện nhằm xác thực nguồn gốc hay chủ sở hữu của đối tượng đó

Khái niệm thủy vân số (..)

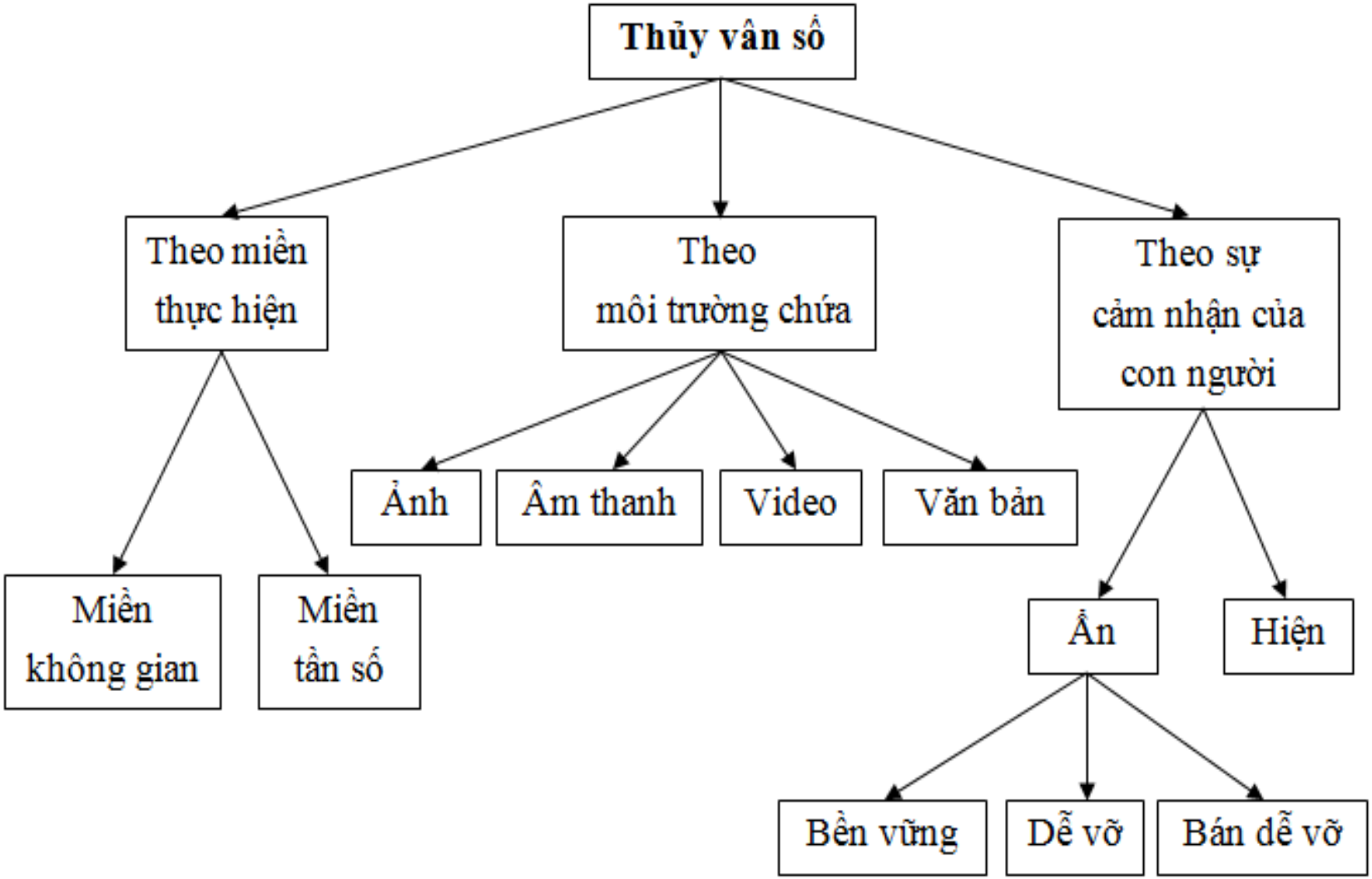
- Ví dụ

Khái niệm thủy vân số (..)

- So sánh với ẩn mã
  - Giống
    - Giấu một dữ liệu vào trong dữ liệu khác
  - Khác về mục đích
    - Ẩn mã: che giấu sự tồn tại của dữ liệu được nhúng
    - Thủy vân: đảm bảo tính xác thực, an toàn và bảo vệ bản quyền đối với dữ liệu chứa thông tin được nhúng

Phân loại thủy vân số

- Có nhiều cách phân loại khác nhau



Cấu trúc của hệ thống thủy vân số

- Kí hiệu:
  - I là vật phủ dung để nhúng thủy vân vào
  - W là thủy vân ban đầu cần nhúng
  - W_e là thủy vân trích xuất được
  - I_W là vật phủ sau khi được nhúng thủy vân
  - K là khóa sử dụng trong quá trình nhúng và phát hiện/ trích xuất thủy vân

Cấu trúc của hệ thống thủy vân số (..)

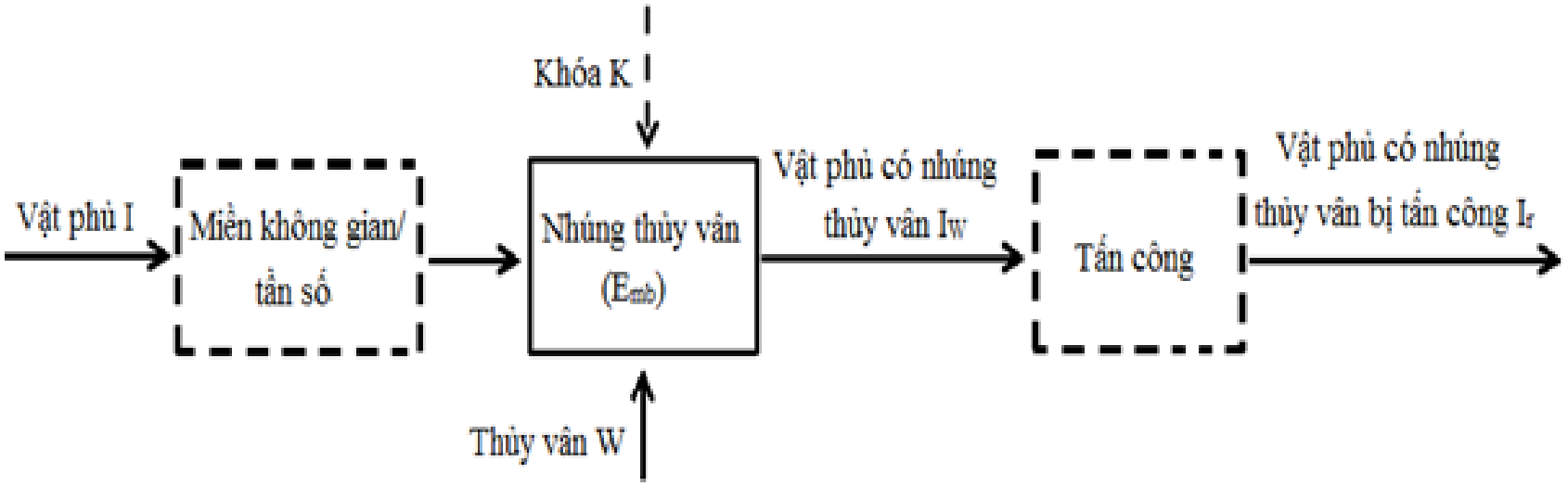
- I_r là vật có nhúng thủy vân nhưng đã bị tấn công trên đường truyền, đây cũng chính là vật dung để kiểm tra trong quá trình phát hiện/trích xuất thủy vân
- E_{mb} là hàm (thuật toán) nhúng thủy vân
- D_{tc} là hàm (thuật toán) trích xuất thủy vân
- D là hàm phát hiện thủy vân
- $f(I)$ là hàm biến đổi vật phủ I sang miền tần số/sóng, giá trị của f là một vector các hệ số tương ứng của vật phủ trên miền lựa chọn

Cấu trúc của hệ thống thủy vân số (..)

- Gồm 2 quá trình:
  - Nhúng thủy vân
  - Phát hiện/trích xuất thủy vân

Cấu trúc của hệ thống thủy vân số (..)

- Quá trình nhúng
  - Nhúng trên miền không gian
    - $E_{mb}(I, W, K) = I_W$
  - Nhúng trên miền tần số
    - $E_{mb}(f(I), W, K) = I_W$
  - Lượcđồnhúngthủyvân

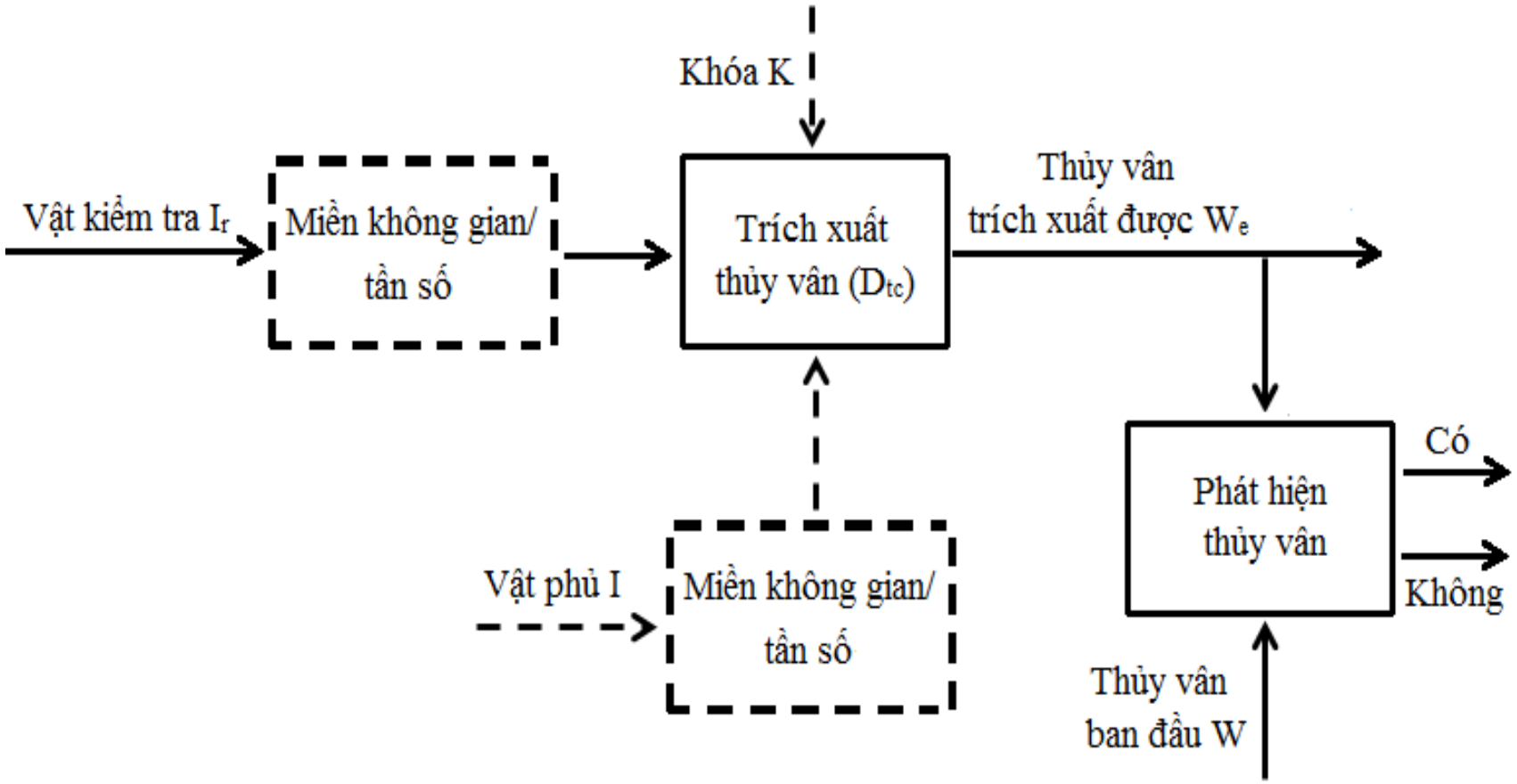


Cấu trúc của hệ thống thủy vân số (..)

- Quá trình phát hiện/trích xuất
  - Nếu quá trình nhúng sử dụng khóa K thì quá trình phát hiện/trích xuất cũng phải áp dụng K
  - Thủy vân mù: $D_{tc}(I_r, K) = W_e$
  - Thủy vân không mù: $D_{tc}(I_r, I, K) = W_e$
  - Quá trình phát hiện mù sinh ra đầu ra là một giá trị nhị phân thể hiện sự có mặt hay không của thủy vân W và có thể được biểu diễn như sau:
    - $D(I_r, W, K) = \begin{cases} 0, không\ có\ thủy\ vân \\ 1, có\ thủy\ vân \end{cases}$

Cấu trúc của hệ thống thủy vân số (..)

- Lược đồ phát hiện/trích xuất thủy vân



Một số tính chất của thủy vân số

- *Bền vững*
  - Không bị thay đổi trước các tác động xử lí cũng như các tấn công
    - Nhưng vẫn có thể phát hiện được sau khi xảy ra các tác động hay tấn công
  - Thường áp dụng trong trường hợp bảo vệ bản quyền chứ không phù hợp với ứng dụng xác thực tính toàn vẹn của dữ liệu

Một số tính chất của thủy vân số (..)

- *Dung lượng nhúng*
  - Là số lượng thông tin có thể được giấu trong vật phủ
  - Luôn phải xem xét tới hai yêu cầu quan trọng khác đó là tính trong suốt và tính bền vững
    - → Để có được dung lượng lớn thường phải mất đi hoặc tính bền vững hoặc tính trong suốt hoặc cả hai

Một số tính chất của thủy vân số (..)

- *Trong suốt (Imperceptibility)*
  - Không thể cảm nhận được bằng các giác quan thông thường của con người về thủy vân đã được nhúng
    - Vẫn phát hiện được thông qua việc xử lí đặc biệt
  - Chỉ áp dụng với thủy vân ẩn chứ không phải thủy vân hiện

Một số tính chất của thủy vân số (..)

- *An toàn*
  - Thủy vân số là dấu hiệu để định danh một cách chính xác
    - → Chỉ những người dùng có thẩm quyền mới có thể phát hiện, trích xuất và thậm chí sửa đổi thủy vân

Sử dụng thủy vân với mục đích bảo vệ bản quyền

Một số tính chất của thủy vân số (..)

- *Chi phí tính toán*
  - Là độ phức tạp của thuật toán sử dụng trong mô hình thủy vân
  - Là vấn đề rất quan trọng đặc biệt trong các ứng dụng giám sát truyền thông
    - Vì việc sản xuất đa phương tiện không được phép chậm và quá trình phát hiện thủy vân phải thực hiện với thời gian thực
  - Cũng là yêu cầu quan trọng đối với các ứng dụng trên các thiết bị di động
    - Vì tài nguyên hạn chế và cần phải cân bằng giữa rất nhiều yếu tố như nguồn pin, băng thông, bộ nhớ, …

Một số kĩ thuật thủy vân số

- Thủy vân trên miền không gian
- Thủy vân trên miền tần số
- Kết hợp thủy vân trên miền không gian và tần số
- Thủy vân dễ vỡ
- Thủy vân bền vững

Một số kĩ thuật thủy vân số (..)

- Thủy vân trên miền không gian
- Thủy vân trên miền tần số
- Kết hợp thủy vân trên miền không gian và tần số
- Thủy vân dễ vỡ
- Thủy vân bền vững

Thủy vân trên miền không gian

- Sửa đổi trực tiếp các giá trị điểm ảnh trên miền không gian của ảnh
- Thường đơn giản và không cần ảnh phủ để trích xuất thủy vân
- Không bền vững đối với các phép xử lí ảnh
  - Vì thủy vân không được phân phối trên toàn bộ ảnh
  - → Các phép xử lí ảnh dễ dàng phá hủy thủy vân

Thủy vân trên miền không gian (..)

- Một số phương pháp:
  - Thay thế
  - Cộng

Thủy vân trên miền không gian (..)

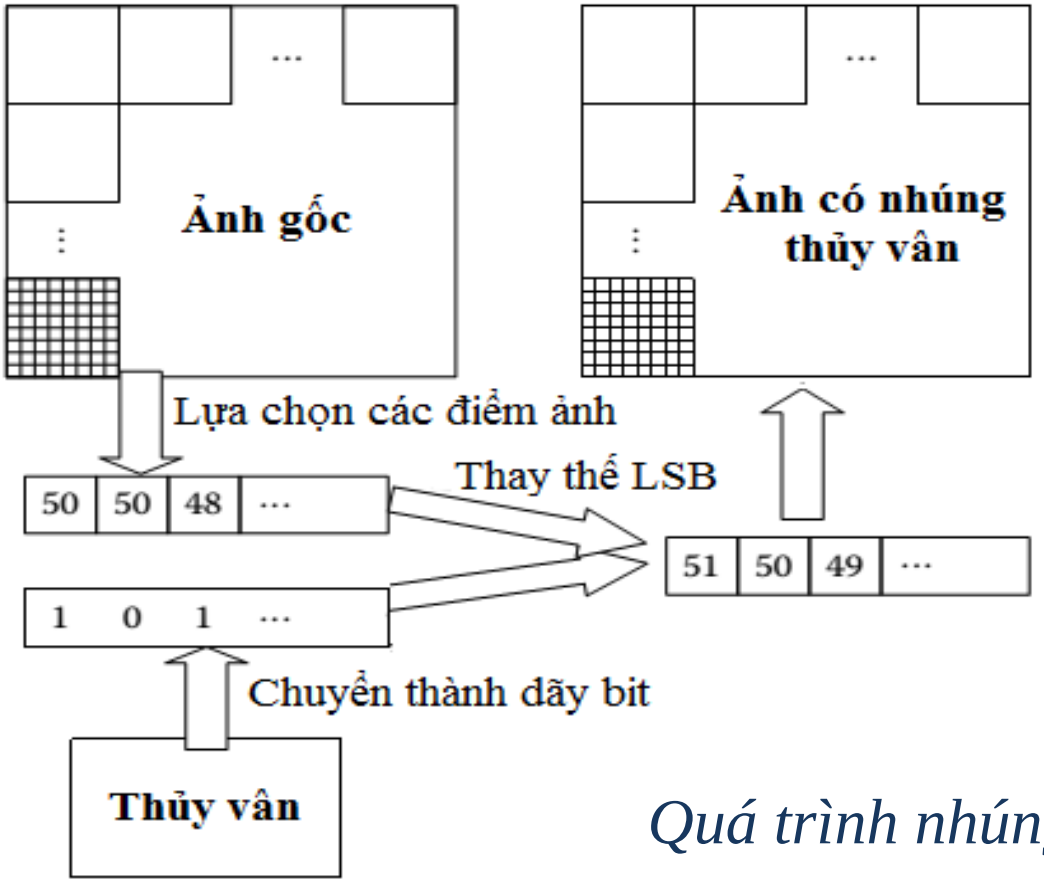
- Một số phương pháp:
  - Thay thế
  - Cộng

Phương pháp thay thế trên miền không gian

- Các vị trí nhúng được xác định trước khi thực hiện nhúng thủy vân
  - → Người nhận cũng biết chính xác các vị trí này
- Quá trình nhúng:
  - Trước tiên, thủy vân được chuyển sang dạng bít
  - Mỗi bít thủy vân được nhúng vào bít cụ thể của các vị trí đã lựa chọn trong ảnh phủ
- Quá trình trích xuất:
  - Người nhận đã biết các vị trí điểm ảnh cụ thể có chứa thủy vân
  - Chuyển mỗi giá trị điểm ảnh sang dạng nhị phân
    - → Thu được các bít thủy vân

Phương pháp thay thế trên miền không gian (..)

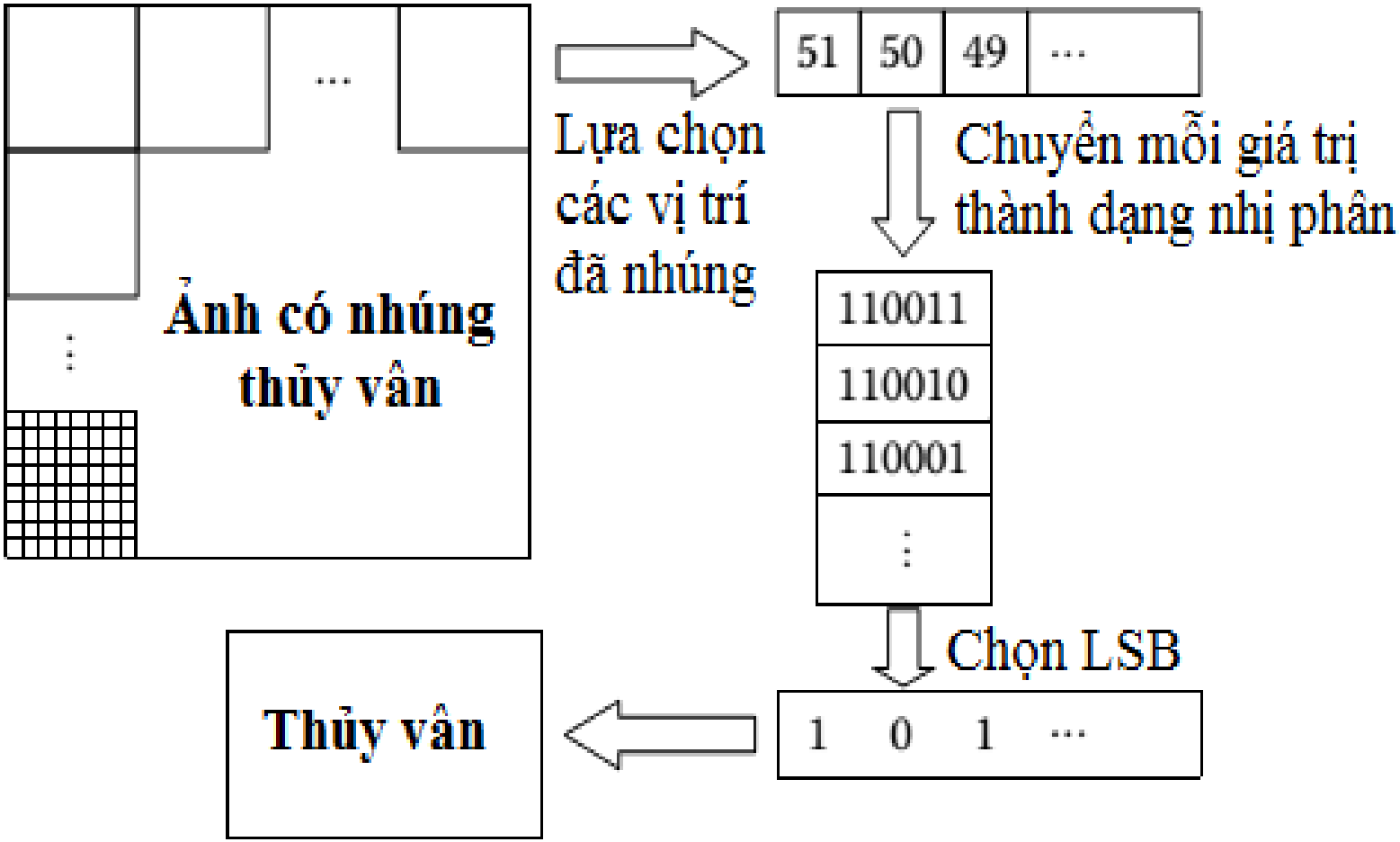
- Ví dụ:
  - Thay thế LSB, với thủy vân là 101 vào các điểm ảnh tương ứng là 50, 50 và 48 của ảnh phủ



Quá trình nhúng

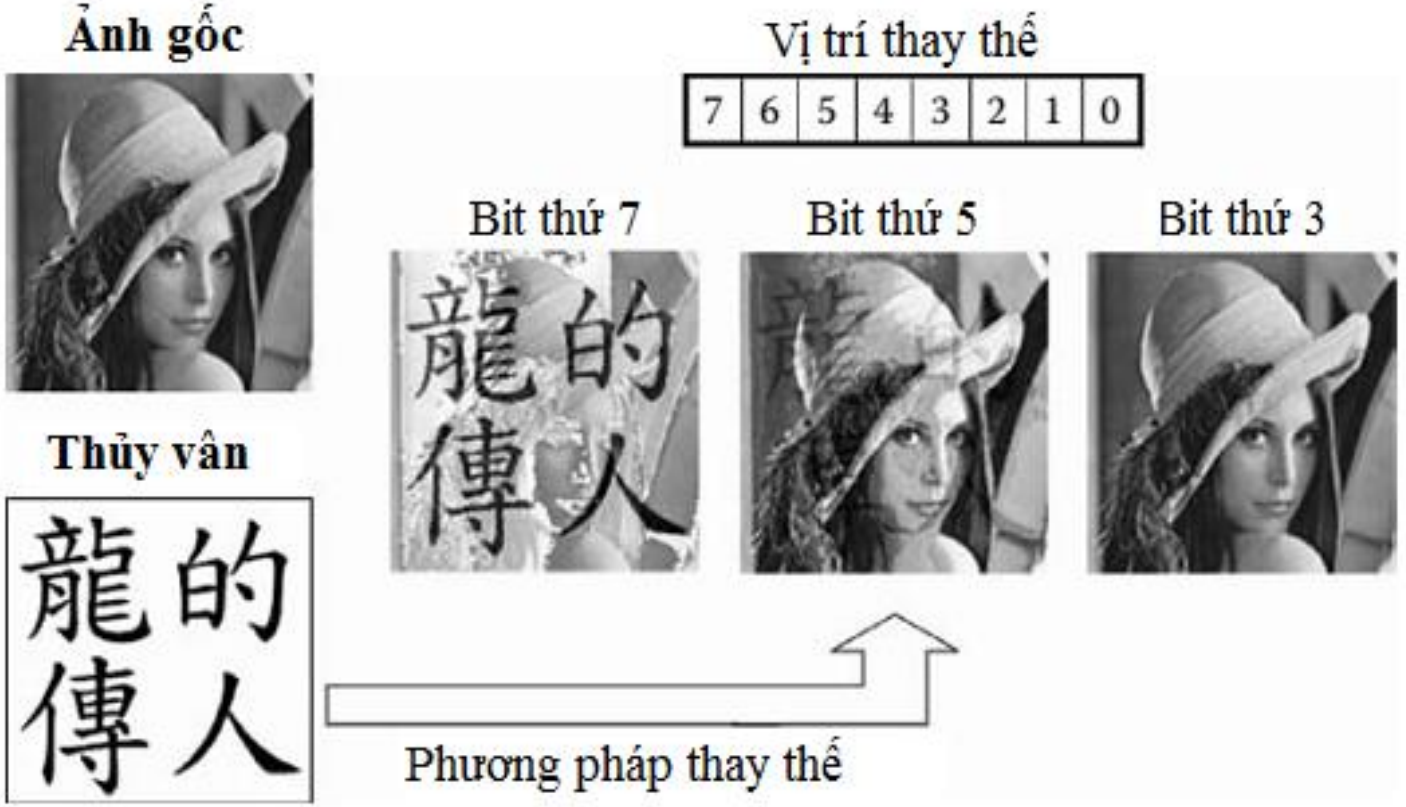
Phương pháp thay thế trên miền không gian (..)

- Quá trình trích xuất:



Phương pháp thay thế trên miền không gian (..)

- Nhúng thủy vân vào các bít khác nhau
  - → Chất lượng ảnh thu được sẽ khác nhau
- Ví dụ:



Phương pháp thay thế trên miền không gian (..)

- Ưu điểm
  - Đơn giản, dễ cài đặt
  - Dung lượng thủy vân thường lớn hơn các cách tiếp cận khác
    - Tối đa có thể lớn gấp 8 lần ảnh phủ
      - Nhưng chất lượng ảnh giảm nghiêm trọng
    - Thường chỉ nên gấp 3 lần ảnh phủ
- Nhược điểm
  - Không bền vững đối với tấn công nén mất dữ liệu, cắt dán ảnh, thêm nhiễu bởi thủy vân bị biến dạng

Phương pháp thay thế trên miền không gian (..)

- ***Thuật toán:***
  - Giả thiết:
    - H là ảnh phủ mức xám có kích thước $N \times N$
    - W là ảnh thủy vân nhị phân kích thước $M \times M$
    - L là số bít được sử dụng trong mức xám của các điểm ảnh.
    - $\oplus$ là phép toán thay thế các bít của thủy vân vào các LSB của ảnh phủ

Phương pháp thay thế trên miền không gian (..)

- *Thuật toán*
  - Lấy các điểm ảnh từ ảnh phủ $H = \{h(i,j), 0 \leq i,j <$

Thủy vân trên miền không gian (..)

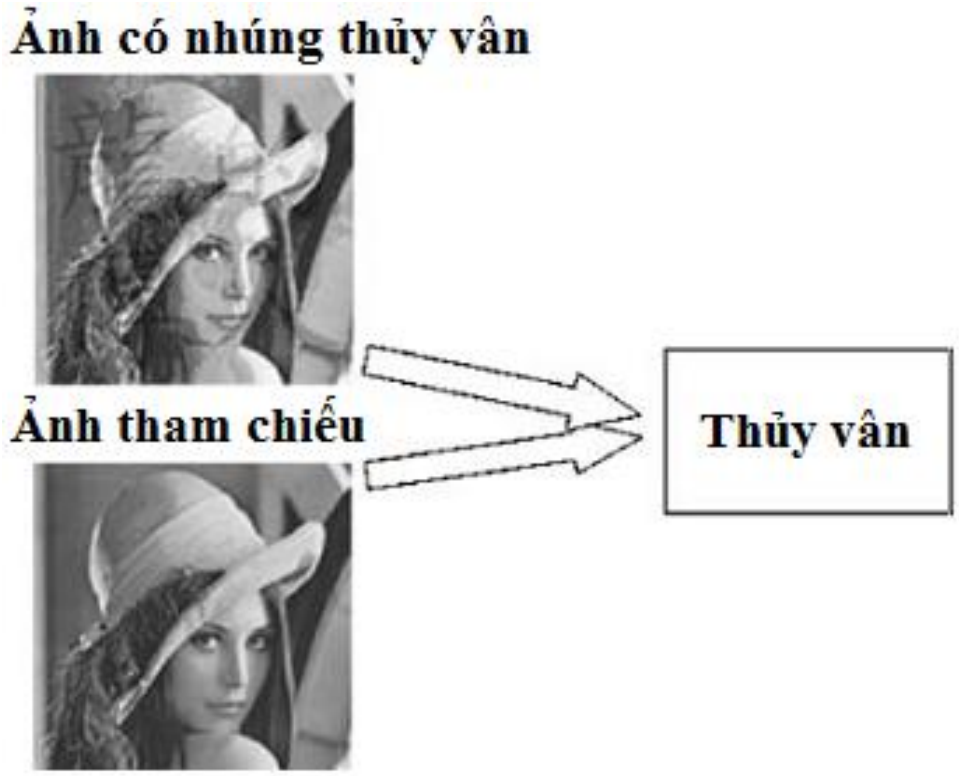
- Một số phương pháp:
  - Thay thế
  - Cộng

Phương pháp cộng trên miền không gian

- Không xét những bít cụ thể của một điểm ảnh
- Cộng một lượng giátrị thủy vân vào một điểm ảnh trong quá trình nhúng
  - $h^*(i,j) = h(i,j) + a(i,j).w(i,j)$, trong đó $\{a(i,j)\}$ là hệ số tỉ lệ
- Nhượcđiểm:
  - $a(i,j)$lớn →ảnh có chứa thủy vân bị méo
    - → Khắc phục:
      - Nhúng một giá trị lớn vào một khối điểm ảnh thay vì một điểm ảnh đơn
      - Trước khi nhúng giá trị thủy vân chia cho kích cỡ khối ảnh để giảm giá trị

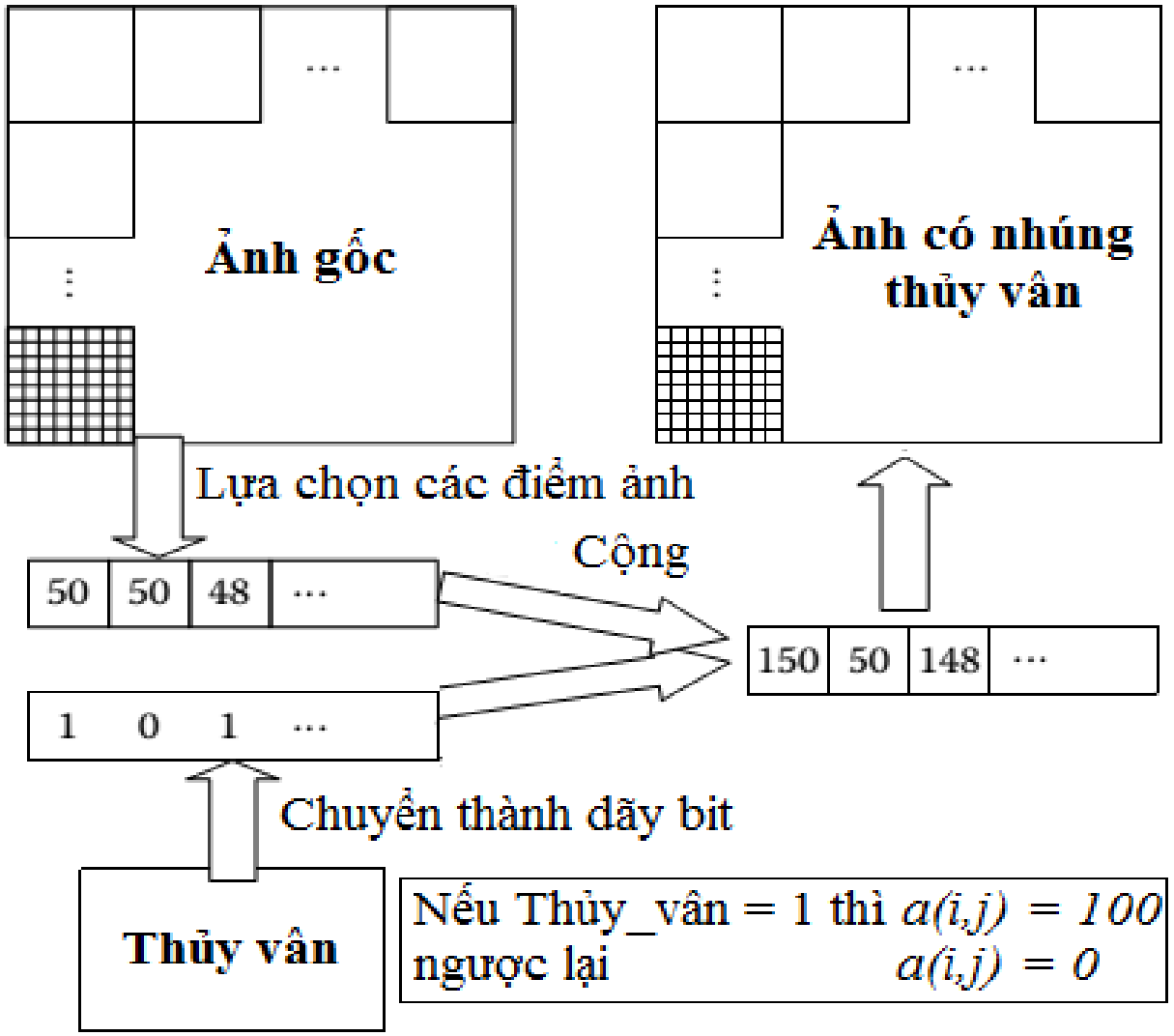
Phương pháp cộng trên miền không gian (..)

- Nhược điểm: (..)
  - Cần ảnh tham chiếu (hay ảnh gốc) khi trích xuất
    - Vì không biết được vị trí đã nhúng nên rất khó có thể xác định được thủy vân



Phương pháp cộng trên miền không gian (..)

- Ví dụ:



Một số kĩ thuật thủy vân số (..)

- Thủy vân trên miền không gian
- Thủy vân trên miền tần số
- Kết hợp thủy vân trên miền không gian và tần số
- Thủy vân dễ vỡ
- Thủy vân bền vững

Thủy vân trên miền tần số

- Điểm ảnh được chuyển sang miền tần số bởi các phép biến đổi:
  - Fourier rời rạc (Discrete Fourier transform – DFT)
  - Cosine rời rạc (Discrete Cosine transform – DCT)
  - Sóng rời rạc (Discrete wavelet transform – DWT)
- Chèn một thủy vân vào các hệ số tần số
  - Thường nhúng vào các thành phần có tần số thấp hoặc các thành phần tần số chứa thông tin quan trọng của ảnh
    - Vì các thành phần tần số cao thường bị mất khi nén hoặc thay đổi kích thước ảnh

Thủy vân trên miền tần số (..)

- So sánh với phương pháp thủy vân trên miền không gian
  - Ưu điểm:
    - Thường bền vững hơn trước các phép biến đổi ảnh
      - Vì năng lượng của ảnh tập trung vào các thành phần có tần số thấp.
      - → Nhúng vào các tần số này thì những biến đổi sẽ được phân phối trên toàn bộ ảnh
  - Nhược điểm:
    - Phức tạp hơn
    - Dung lượng nhúng ít hơn

Thủy vân trên miền tần số (..)

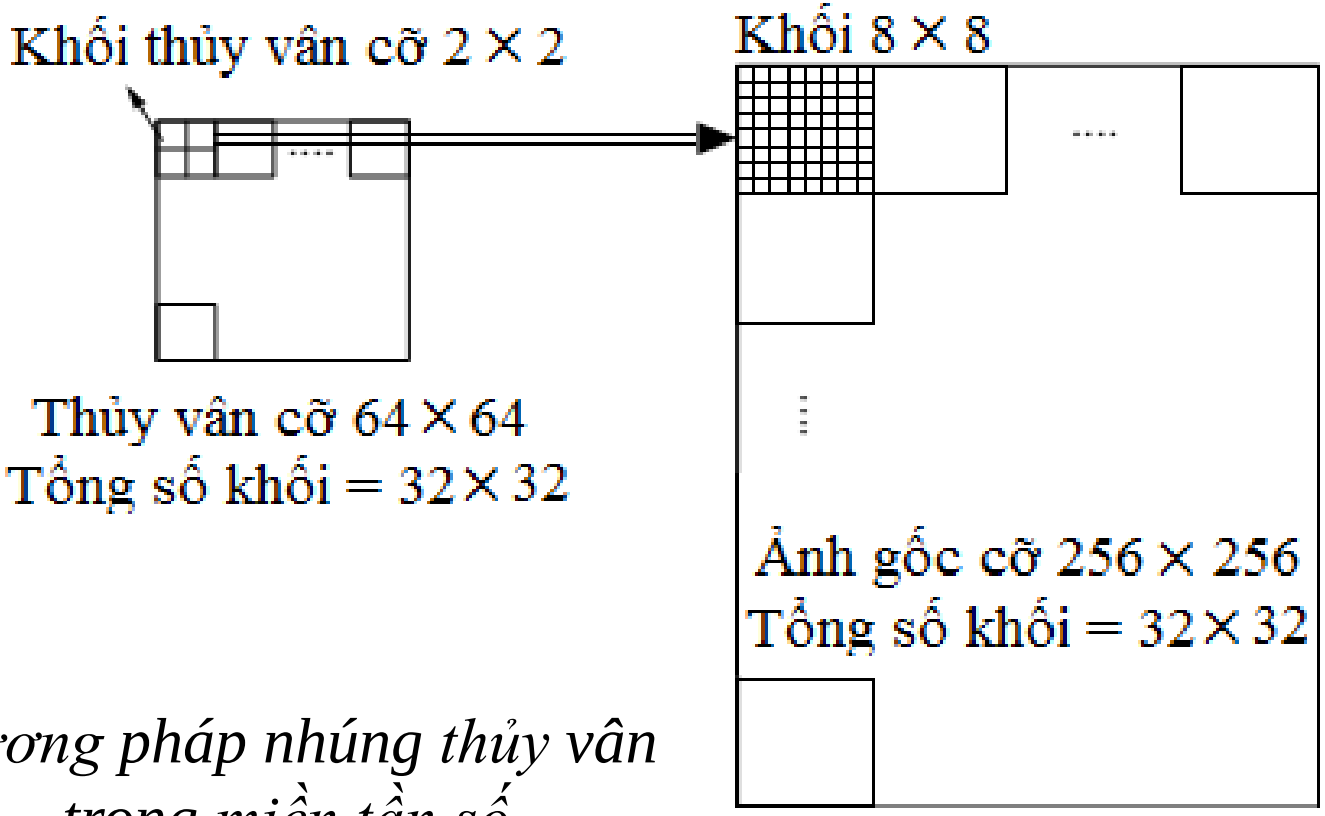
- Một số phương pháp:
  - Thay thế
  - Nhân

Thủy vân trên miền tần số (..)

- Một số phương pháp:
  - Thay thế
  - Nhân

Phương pháp thay thế trên miền tần số (..)

- Về cơ bản giống với trong miền không gian
  - Nhưng nhúng thủy vân vào các hệ số tần số



Phương pháp nhúng thủy vân trong miền tần số

Phương pháp thay thế trên miền tần số (..)

- ***Thuật toán:***
  - Giả thiết:
    - Cho H^m và W^n tương ứng là các ảnh được chia nhỏ ra từ ảnh phủ H cỡ $N \times N$ và thủy vân W cỡ $M \times M$
    - H^{m_DCT} là ảnh sau khi biến đổi H^m bởi phép DCT
    - H^{m_F} là ảnh sau khi nhúng W^n vào H^{m_DCT}

Phương pháp thay thế trên miền tần số (..)

□ *Thuật toán:*

- Chia ảnh phủ thành các khối ảnh có kích thước 8×8

$8H = \{h(i,j), 0 \le i,j < N\}$,

$H^m = \{h^m(i,j), 0 \le i,j < 8\}$,

$trong$ đó $h^m(i,j) \in \{0,1,2,\dots,2^L - 1\}$

$và\ m\ là\ tổng\ số\ các\ khối\ 8 \times 8$

- Chia ảnh thủy vân thành các khối ảnh có kích thước 2×2

$W = \{w(i,j), 0 \le i,j < M\}$

$W^n = \{w^n(i,j), 0 \le i,j < 2\}$,

$trong$ đó $w^n(i,j) \in \{0,1\}$

$và\ n\ là\ tổng\ số\ khối\ 2 \times 2$

Phương pháp thay thế trên miền tần số (..)

- *Thuật toán: (..)*
  - Sử dụng công thức DCT để chuyển H^m thành H^{m_DCT}
  - Chèn W^m vào các hệ số của H^{m_DCT}

H^{m_F}

$= \{h^{m\_F}(i,j) = h^{m\_DCT}(i,j) \oplus w^m(i,j), 0 \leq i,j < 8\}$

  - Áp dụng phép biến đổi DCT ngược để chuyển ảnh có chứa thủy vân H^{m_F} về dạng ảnh thông thường

Phương pháp thay thế trên miền tần số (..)

- Ví dụ:
  - Nhúng thủy vân 4 bít vào miền tần số của ảnh.
    - Hình(a) là một ảnh gốc mức xám có kích thước 8×8
    - Hình(b) là ảnh đã được biến đổi bởi DCT
    - Hình(c) là thủy vân nhị phân:
      - 0 và 1 là các giá trị được nhúng
      - Dấu gạch nối (-): không thay đổi ở vị trí đó
    - Hình (d) là kết quả sau khi nhúng thủy vân ở hình (c) vào ảnh đã được biến đổi (b) bằng cách dung phép thay thế LSB

Phương pháp thay thế trên miền tần số (..)

- Ví dụ: (..)

1	8	219	51	69	171	81	41
94	108	20	121	17	214	15	74
233	93	197	83	177	215	183	78
41	84	118	62	210	71	122	38
222	73	197	248	125	226	210	5
35	36	127	5	151	2	197	165
196	180	142	52	173	151	243	164
254	62	172	75	21	196	126	224

(a) Ảnh gốc

DCT

970.50	−42.37	−4.99	94.09	−94.25	82.58	115.99	96.96
−144.74	30.63	−165.94	22.53	−55.09	−26.76	45.39	−76.50
−46.77	−28.71	113.62	−40.93	−28.33	−39.12	131.28	−87.92
−88.67	−60.13	−70.12	−84.05	−38.84	18.38	−54.63	53.37
−14.75	32.48	−88.16	−27.56	−18.00	72.99	76.57	−12.66
−1.06	−37.05	−19.76	−24.91	−41.49	−91.99	−76.61	171.35
−16.89	−47.45	24.28	−56.94	−0.44	20.51	59.88	133.33
222.41	79.21	−18.53	92.78	−46.48	123.71	58.15	−18.58

(b) Ảnh được biến đổi

-	-	0	1	-	-	-	-
-	1	-	-	-	-	-	-
1	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-

(c) Thủy vân được nhúng

970.50	−42.37	−4.99	95.09	−94.25	82.58	115.99	96.96
−144.74	31.63	−165.94	22.53	−55.09	−26.76	45.39	−76.50
−47.77	−28.71	113.62	−40.93	−28.33	−39.12	131.28	−87.92
−88.67	−60.13	−70.12	−84.05	−38.84	18.38	−54.63	53.37
−14.75	32.48	−88.16	−27.56	−18.00	72.99	76.57	−12.66
−1.06	−37.05	−19.76	−24.91	−41.49	−91.99	−76.61	171.35
−16.89	−47.45	24.28	−56.94	−0.44	20.51	59.88	133.33
222.41	79.21	−18.53	92.78	−46.48	123.71	58.15	−18.58

(d) Ảnh biến đổi có nhúng thủy vân

Phương pháp thay thế trên miền tần số (..)

- Ví dụ: (..)
  - Cách nhúng thủy vân vào các hệ số của ảnh biến đổi

W	Hệ số ban đầu	Phần nguyên	Nhị phân	Đã nhúng thủy vân	
				Nhị phân	Hệ số
1	-46.77	46	00101110	00101111	-47.77
1	30.63	30	00011110	00011111	31.63
0	-4.99	4	00000100	00000100	-4.99
1	94.09	94	01011110	01011111	95.09

Thủy vân trên miền tần số (..)

- Một số phương pháp:
  - Thay thế
  - Nhân

Phương pháp nhân trên miền tần số

- Chèn thủy vân vào một vùng đã xác định trước của các tần số trong ảnh đã biến đổi
  - Thường là vùng quan trọng đối với việc nhận thức về sự thay đổi (hay chính là thành phần tần số quan trọng) của ảnh
    - → Chống lại được các tấn công.
- Thủy vân được thu nhỏ theo độ lớn của thành phần tần số đặc biệt
- Thủy vân chứa một chuỗi phân bố Gauss ngẫu nhiên

Phương pháp nhân trên miền tần số (..)

- Giảsử:
  - H là các hệ số DCT của ảnh gốc
  - W là vector ngẫu nhiên thì
    - $\{h(m,n)\}$ và $\{w(i)\}$ biểu thị các điểm ảnh tương ứng của H và W
- Phép nhúng W vào H để thu được ảnh có thủy vân H^* có thể sử dụng công thức sau: $h^*(m,n) = h(m,n)\big(1 + \alpha(i)\,.w(i)\big)$
  - $\{\alpha(i)\}$ lớn thì ảnh có chứa thủy vân sẽ bị méo nhiều hơn
  - Thường $\{\alpha(i)\} = 0.1$ để cân bằng được tính trong suốt và bền vững

Phương pháp nhân trên miền tần số (..)

- Công thức trích xuất:

$$w'(i) = \frac{h^*(m,n) - h(m,n)}{\alpha(i) \,.\, h(m,n)}$$

Một số kĩ thuật thủy vân số (..)

- Thủy vân trên miền không gian
- Thủy vân trên miền tần số
- Kết hợp thủy vân trên miền không gian và tần số
- Thủy vân dễ vỡ
- Thủy vân bền vững

Kết hợp thủy vân trên miền không gian và tần số

- Được đưa ra nhằm giải quyết nhược điểm của hai phương pháp thủy vân trên miền không gian và tần số
- Ý tưởng:
  - Tách ảnh thủy vân ra thành hai phần
  - Chèn trong miền không gian và tần số dựa trên sự ưu tiên của người dùng và mức độ quan trọng của dữ liệu

Kết hợp thủy vân trên miền không gian và tần số (..)

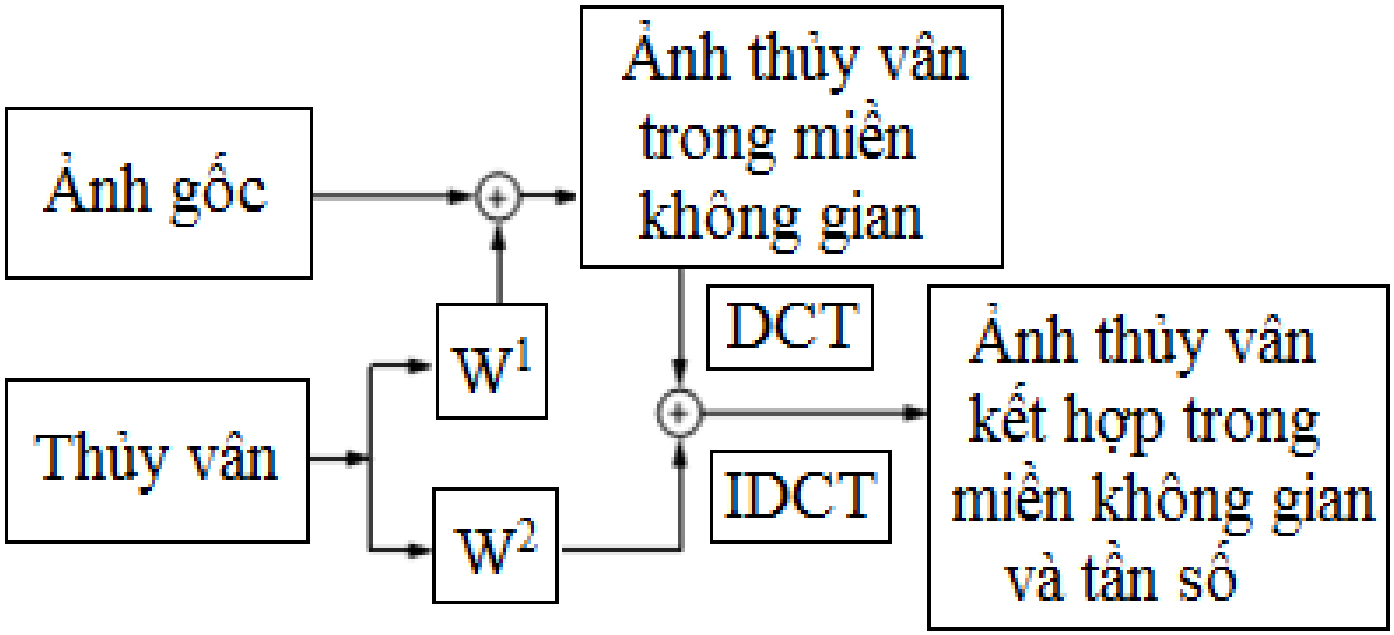
- Phụ thuộc vào yêu cầu của người dùng và phụ thuộc vào ứng dụng trong việc phân tách ảnh thủy vân thành hai phần để chèn vào miền không gian và miền tần số
  - Về nguyên tắc, thông tin quan trọng nhất xuất hiện ở phần trung tâm của ảnh
    - → Cách tách đơn giản là lựa chọn cửa sổ trung tâm trong ảnh thủy vân và chèn phần này vào miền tần số
    - Theo sự ưu tiên của người dùng thì có thể cắt dữ liệu bí mật nhất để chèn vào miền tần số

Kết hợp thủy vân trên miền không gian và tần số (..)

- Giả sử:
  - H là ảnh phủ mức xám có kích thước $N \times N$
  - W là ảnh thủy vân ở dạng nhị phân có kích thước $M \times M$
  - W^1 và W^2 là hai thủy vân được tách ra từ W
  - H^S là ảnh kết hợp từ H và W^1trong miền không gian
  - H^{DCT} là ảnh trong đó H^S được biến đổi sang miền tần số theo phép biến đổi DCT
  - H^F là ảnh nhận được khi kết hợp H^{DCT} và W^2trong miền tần số
  - $\bigoplus$ là phép toán thay thế các bít của thủy vân vào các LSB của ảnh phủ

Kết hợp thủy vân trên miền không gian và tần số (..)

- ***Thuật toán:***
  - Sơ đồ luồng



Kết hợp thủy vân trên miền không gian và tần số (..)

- *Thuật toán*
  - Tách thủy vân thành hai phần: $W = \{w(i,j), 0 \leq i,j <$

Kết hợp thủy vân trên miền không gian và tần số (..)

- *Thuật toán: (..)*
  - Biến đổi H^S thành H^{DCT} theo phép biến đổi DCT
  - Chèn W^2 vào các hệ số của H^{DCT} thành $H^F H^F = \{h^F(i,j) = h^{DCT}(i,j) \oplus w^2(i,j), 0 \le i,j < N\}$, $trong$ đó $h^F(i,j) \in \{0,1,2,\dots,2^L - 1\}$
  - Biến đổi ảnh có nhúng thủy vân ở dạng DCT về dạng bình thường bằng phép biến đổi DCT ngược

Một số kĩ thuật thủy vân số (..)

- Thủy vân trên miền không gian
- Thủy vân trên miền tần số
- Kết hợp thủy vân trên miền không gian và tần số
- Thủy vân dễ vỡ
- Thủy vân bền vững

Thủy vân dễ vỡ

- Xử lí ảnh dựa trên máy tính ngày càng phổ biến nên có rất nhiều công cụ phần mềm hỗ trợ
  - → Cần phải đánh giá được liệu ảnh nhận được có bị sửa đổi trong quá trình truyền tin hay không
  - Thủy vân dễ vỡ giải quyết được vấn đề này
    - Vì sau khi được nhúng vào ảnh phủ nó dễ dàng bị thay đổi nếu có bất cứ tác động nào lên ảnh
    - → Chỉ cần đánh giá thủy vân được giấu trong ảnh sẽ biết được ảnh có bị biến đổi hay không

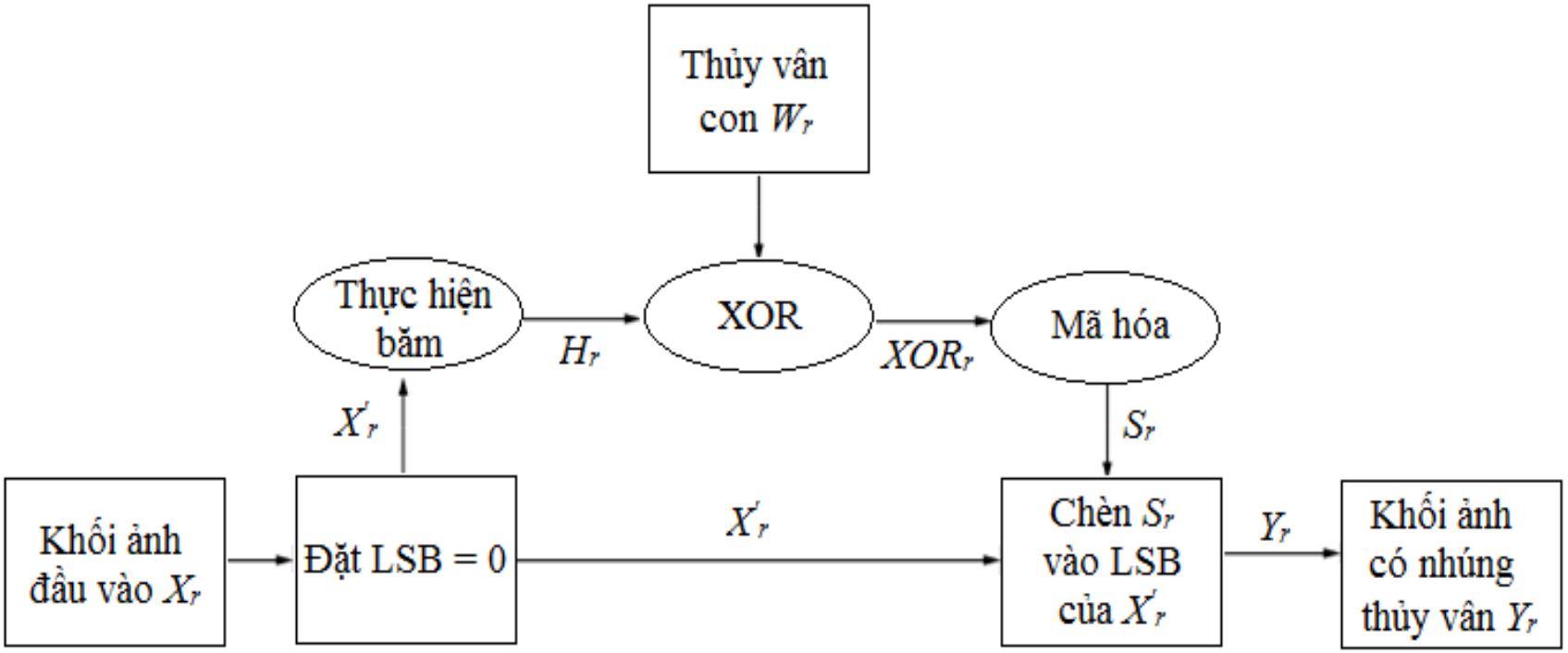
Phát hiện bất kì sự sửa đổi trái phép trong quá trình liên lạc

Thủy vân dễ vỡ (..)

- Wong đã giới thiệu thuật toán thủy vân dễ vỡ dựa trên khối
  - Nhằm phát hiện ra những thay đổi của ảnh như các giá trị điểm ảnh, kích cỡ ảnh
  - Sử dụng thuật mã hóa khóa công khai RSA và hàm băm MD5

Thủy vân dễ vỡ (..)

- ***Thuật toán nhúng:***
  - *Sơ đồ:*

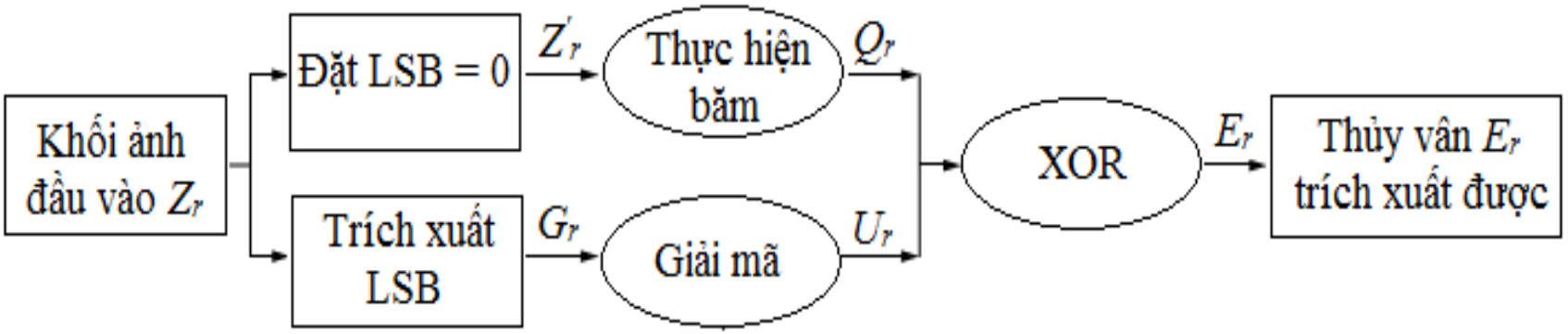


Thủy vân dễ vỡ (..)

- *Thuật toán:*
  - Chia ảnh X thành các ảnh con X_r
  - Chia thủy vân W thành các thủy vân con W_r
  - Với mỗi ảnh con X_r, đặt LSB thành bít 0 để nhận được X_r'
  - Với mỗi X_r', dung hàm băm (ví dụ MD5 hoặc SHA) để nhận được mã băm H_r
  - XOR_r là kết quả nhận được khi thực hiện XOR H_rvới W_r
  - Mã hóaXOR_rbằng thuật toán RSA với khóa riêng K' để nhận được S_r
  - Nhúng $S_r$vào LSB của X_r' để thu được ảnh con có thủy vân Y_r

Thủy vân dễ vỡ (..)

- ***Thuật toán trích xuất:***
  - *Sơ đồ:*



Thủy vân dễ vỡ (..)

- ***Thuật toán trích xuất:***
  - *Thuật toán:*
    - Chia ảnh Z nhận được thành các ảnh con Z_r
    - Đặt LSB của Z_r thành bít 0 kết quả thu được là Z'_r
    - Trích xuất LSB của Z_r nhận được G_r
    - Giải mã G_r bằng cách dùng RSA với khóa công khai K để thu được U_r
    - Với mỗi Z'_r sử dụng hàm băm để nhận được mã băm tương ứng Q_r
    - XOR Q_r với G_r để trích xuất thủy vân E_r

Một số kĩ thuật thủy vân số (..)

- Thủy vân trên miền không gian
- Thủy vân trên miền tần số
- Kết hợp thủy vân trên miền không gian và tần số
- Thủy vân dễ vỡ
- Thủy vân bền vững

Thủy vân bền vững

- Có khả năng đảm bảo an toàn cho dữ liệu như một biện pháp bảo vệ bản quyền
  - Thủy vân vẫn tồn tại dù có bị tấn công:
    - Ví dụ: nén JPEG, nhiễu Gaussian, lọc thông thấp
- Thường có hai cách tiếp cận:
  - Khai thác thông tin dư thừa
  - Dựa trên trải phổ

Thủy vân bền vững (..)

- Khai thác thông tin dư thừa
  - Nhúng nhiều bản sao của cùng một thủy vân vào trong ảnh gốc
    - Ảnh gốc được chia ảnh thành các khối phân biệt sao cho không chồng lên nhau
    - Xử lí riêng từng khối
- → Chống lại kiểu tấn công cắt xén

Thủy vân bền vững (..)

- Dựa trên trải phổ
  - Nhúng dữ liệu trải khắp ảnh (trải qua nhiều tần số)
    - Ảnh gốc được chuyển sang miền tần số
    - Nhúng thủy vân vào các vị trí mà hệ số có ý nghĩa (hệ số có giá trị tuyệt đối lớn)
- → Hầu như bền vững trước các thao tác xử lí ảnh thông thường

Thủy vân bền vững (..)

- Nhận xét:
  - Dung lượng nhúng của hầu hết các thuật toán thủy vân bền vững không cao
    - Khai thác thông tin dư thừa:
      - Do phải nhúng nhiều bản sao của thủy vân vào trong ảnh nên kích thước của từng thủy vân riêng lẻ phải bị hạn chế
    - Dựa trên trải phổ:
      - Do số lượng các hệ số ý nghĩa không nhiều
- → Khi xây dựng các thuật toán thủy vân bền vững thường quan tâm tới vấn đề **cải thiện dung lượng nhúng**

Một số phương pháp tấn công thủy vân số

- Tấn công xử lí hình ảnh
- Tấn công chuyển đổi hình học
- Tấn công mật mã
- Tấn công giao thức

Một số phương pháp tấn công thủy vân số

- Tấn công xử lí hình ảnh
- Tấn công chuyển đổi hình học
- Tấn công mật mã
- Tấn công giao thức

Tấn công xử lí hình ảnh

- Nhằm loại bỏ hoàn toàn thông tin thủy vân ra khỏi dữ liệu có chứa thủy vân mà không phá hủy tính an toàn của thuật toán nhúng thủy vân
  - Ví dụ: không biết khóa được sử dụng để nhúng thủy vân
- Tốn nhiều chi phí tính toán và thậm chí không thể khôi phục lại các thông tin thủy vân từ các dữ liệu bị tấn công

Tấn công xử lí hình ảnh (..)

- Gồm:
  - Tấn công bằng lọc
  - Tấn công bằng tái điều chế
  - Tấn công bằng cách làm biến dạng mã hóa JPEG
- Các phương pháp tấn công này có thể không loại bỏ hoàn toàn thủy vân, nhưng vẫn có thể gây hại đáng kể đến thông tin thủy vân

Một số phương pháp tấn công thủy vân số

- Tấn công xử lí hình ảnh
- Tấn công chuyển đổi hình học
- Tấn công mật mã
- Tấn công giao thức

Tấn công chuyển đổi hình học

- Không thực sự loại bỏ thủy vân
  - Nhằm làm biến dạng nó thông qua sự thay đổi không gian hay thời gian của dữ liệu thủy vân
- Thường làm mất sự đồng bộ giữa máy phát hiện thủy vân và các thông tin thủy vân được nhúng
  - Các máy phát hiện có thể khôi phục lại các thông tin thủy vân nhúng khi sự đồng bộ hóa hoàn hảo được thực hiện
  - Tuy nhiên, trong thực tế quá trình đồng bộ có thể rất phức tạp và không thể áp dụng được

Tấn công chuyển đổi hình học (..)

- Gồm: Co dãn, xoay, cắt, chuyển đổi tuyến tính, uốn, cong vênh, chiếu phối cảnh, cắt dán và lấy mẫu

Một số phương pháp tấn công thủy vân số

- Tấn công xử lí hình ảnh
- Tấn công chuyển đổi hình học
- Tấn công mật mã
- Tấn công giao thức

Tấn công mật mã

- Bẻ gãy tính an toàn của hệ thống thủy vân và tìm cách loại bỏ thông tin thủy vân được nhúng vào hay tìm cách nhúng thủy vân giả

Tấn công mật mã (..)

- Một số phương pháp:
  - Tìm kiếm khóa đầy đủ:
    - Cố gắng tìm kiếm khóa được sử dụng khi nhúng
    - Tìm được khóa thì thủy vân sẽ bị ghi đè
  - Tấn công Oracle:
    - Cố gắng tạo ra một ảnh không có thủy vân cho một thiết bị phát hiện thủy vân có sẵn
    - Tập dữ liệu tấn công được tạo ra bằng cách kết hợp các phần nhỏ của mỗi tập dữ liệu và thiết lập một bộ dữ liệu mới để tấn công
      - Thay đổi dần dần tới khi bộ trích xuất không thể tìm thấy nó nữa

Một số phương pháp tấn công thủy vân số

- Tấn công xử lí hình ảnh
- Tấn công chuyển đổi hình học
- Tấn công mật mã
- Tấn công giao thức

Tấn công giao thức

- Tạo ra giao thức không rõ ràng trong quá trình thủy vân
- Có 2 loại:
  - Tấn công nghịch đảo
  - Tấn công sao chép

Tấn công giao thức (..)

- Tấn công nghịch đảo:
  - Dựa trên cơ chế thủy vân có thể đảo ngược
    - Kẻ tấn công có thể tuyên bố là chủ sở hữu của dữ liệu
      - Vì dữ liệu cũng chứa thủy vân của kẻ tấn công khi trích xuất ra thủy vân của chính anh ấy/cô ấy
      - Tạo ra sự không rõ ràng trong việc xác định người chủ bản quyền
      - → Giải pháp cho vấn đề này là tạo thủy vân từ hàm một chiều