HỌC VIỆN KỸ THUẬT MẬT MÃ

Khoa An Toàn Thông Tin

Bộ môn Khoa Học An Toàn Thông Tin

******

Kĩ Thuật Giấu Tin

Nội dung môn học

1. Tổng quan về giấu tin
2. **Ẩn mã**
3. Phân tích ẩn mã
4. Thủy vân số

Chương 2. Ẩn mã

Chương 2. Ẩn mã

Giới thiệu

STEGANOGRAPHY

History:

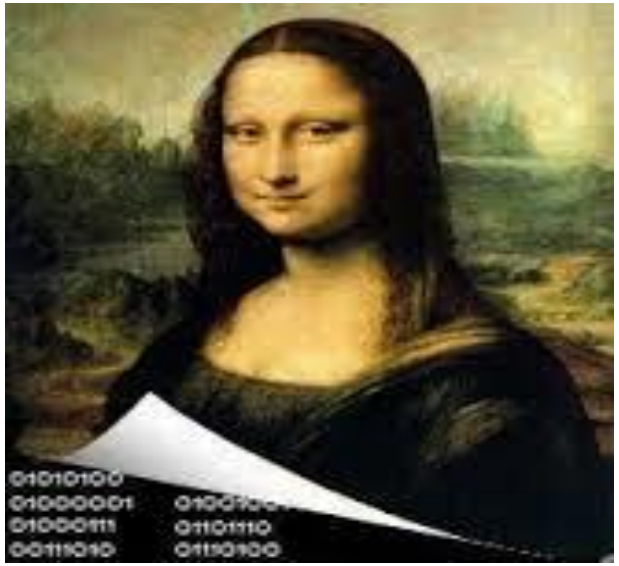
EXAMPLE NOTED BY HERODOTUS :

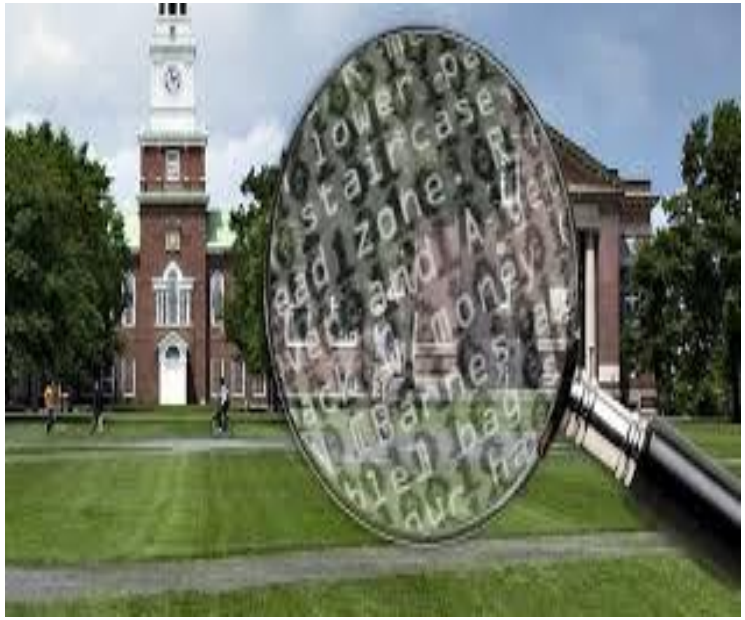
Histiaios, being himself detained, wished to inform Aristagoras that he should revolt. Therefore he shaved the hair of a faithful servant and tattooed his head.

once his hair had grown back, the slave traveled to Mileots where he had his head re-shaved and thus message was retrieved.

Giới thiệu


ngah di SD Nege
ati. Menamatkan SM
1996. Menempuh
Perguruan Islam (API)
t Alfiyah Ibnu Malik lulus
Malindo Irfan, PT. Yo
Harmony Cassette
pernah pula






We Are Ready to Attack the Parliament House
Terrorists use the technique of Steganography to Send and Receive Messages

Chương 2. Ẩn mã

Khái niệm ẩn mã

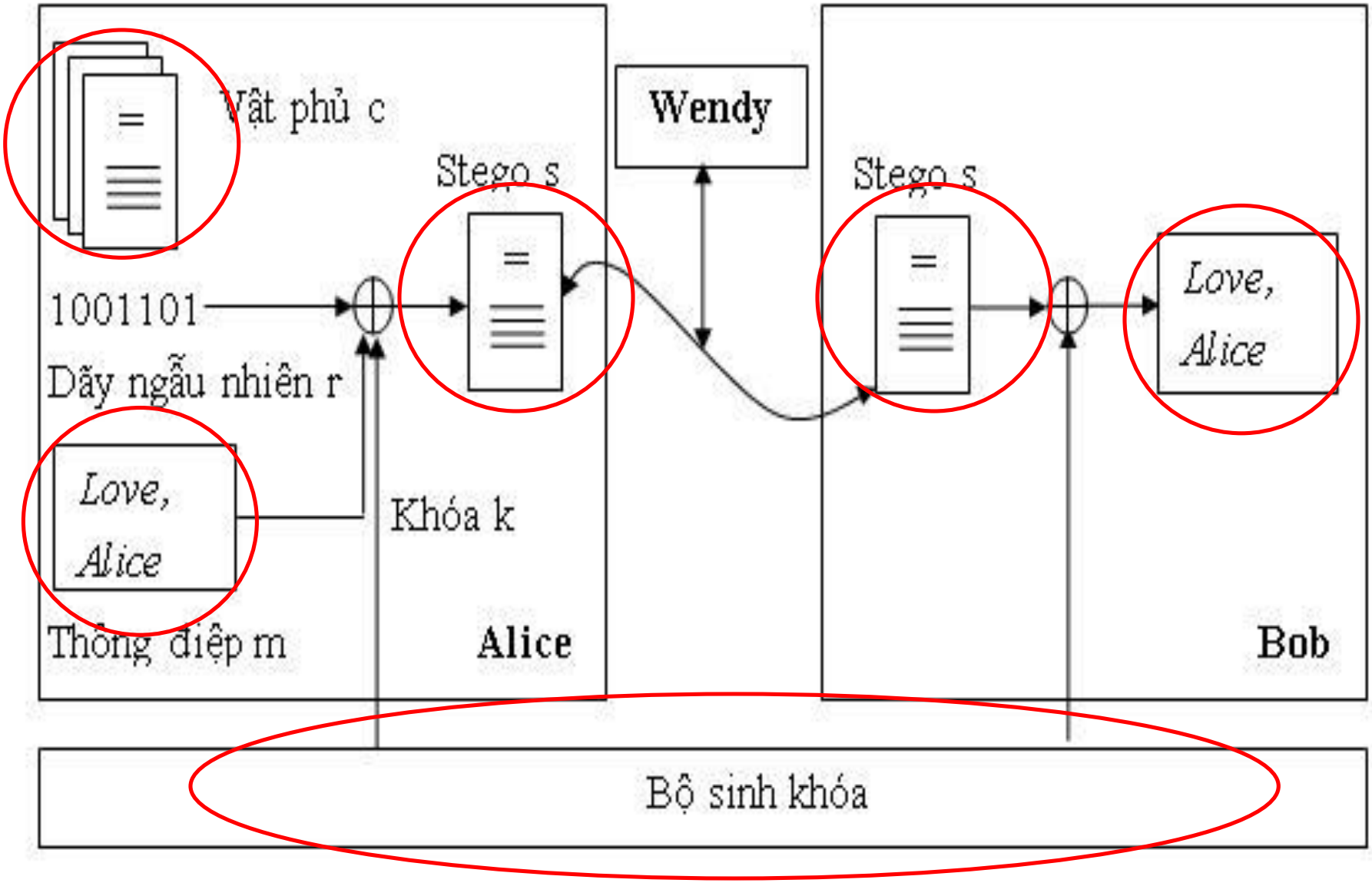
- Ẩn mã học là một nghệ thuật và khoa học của việc truyền thông tin bí mật theo cách không phát hiện ra chính sự tồn tại của thông tin bí mật đó

Khái niệm ẩn mã (..)

- Đối tượng được dùng để ẩn mã (cover object) gọi là môi trường chứa, vật chứa, vật phủ, vật gốc, …
  - Thường dùng ảnh số, âm thanh số, văn bản, kênh liên lạc số hóa …
- Vật sau khi được ẩn mã gọi là vật mang tin hay vật ẩn mã, … (stego object)
  - Vật phủ và vật ẩn mã có bề ngoài không khác nhau

Chương 2. Ẩn mã

Các nguyên lí của ẩn mã



Các nguyên lí của ẩn mã

- ***Định nghĩa 2.1*** (Ẩn mã thuần tuý)
  - Bộ bốn $\sigma = (C, M, D, E)$, trong đó C là tập các vật phủ có thể, M là tập các thông điệp mật với $|C| \geq |M|$
    - $E: C \times M \rightarrow C$ là hàm nhúng tinvà
    - $D: C \rightarrow M$ là hàm trích xuất tin với tính chất:

    $D\big(E(c, m)\big) = m$ với $\forall\, m \in M$ và $c \in C$ được gọi là hệ ẩn mã thuần tuý

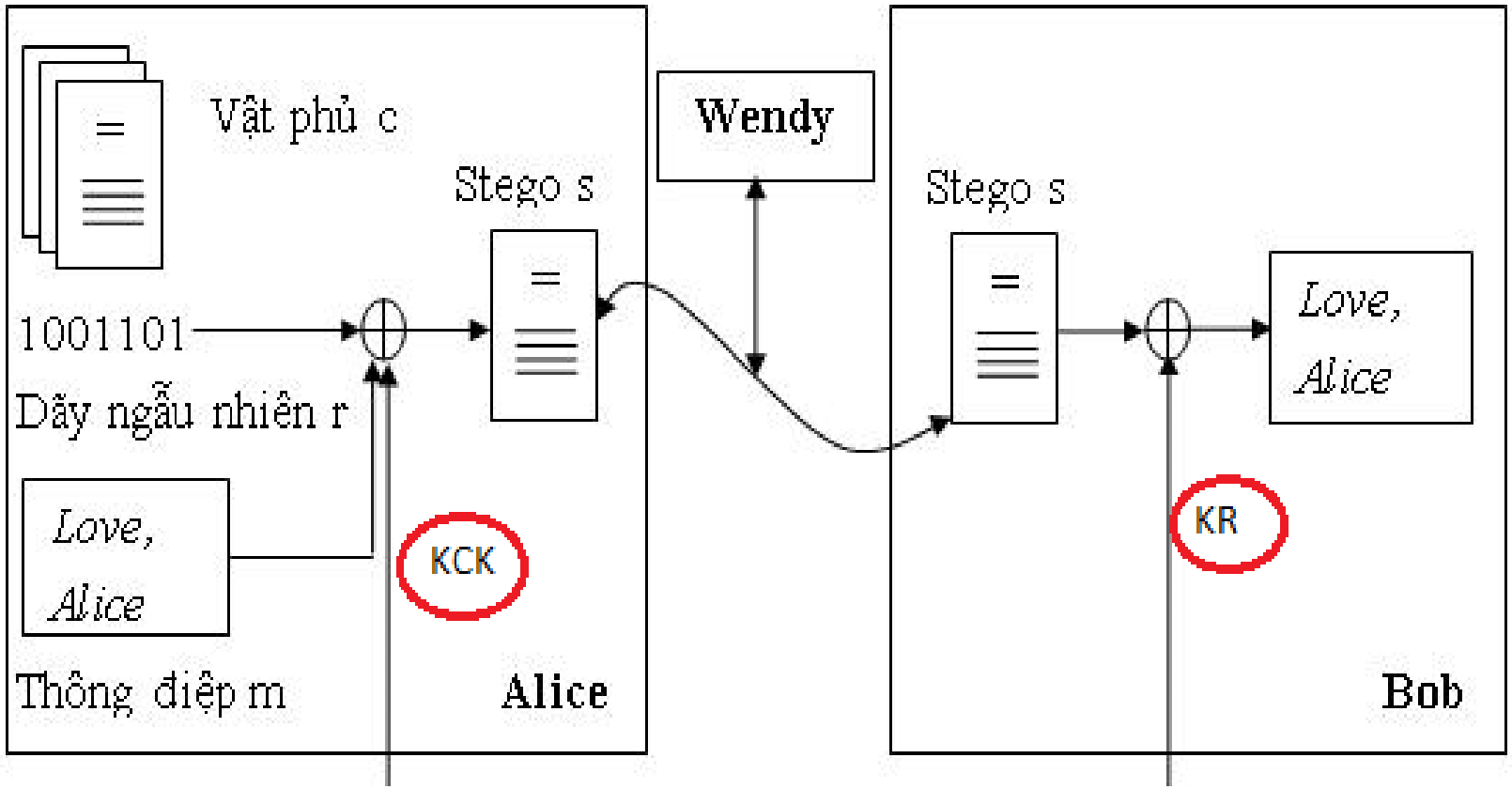
Các nguyên lí của ẩn mã

- ***Địnhnghĩa 2.3*** *(Ẩn mã khoá bí mật)*
  - Bộ năm $\sigma = (C, M, K, D_K, E_K)$, trong đó C là tập các vật phủ có thể, M là tập các thông điệp mật với$|C| \geq |M|$, K là tập các khoá bí mật.
    - Hàm nhúng E_K: $C \times M \times K \rightarrow C$ và
    - Hàm trích xuất D_K: $C \times K \rightarrow M$với tính chất:

    $D_K(E_K(c, m, k), k) = m$với$\forall m \in M$ và c $\in C$ và $k \in K$ được gọi là một hệ ẩn mã khoá bí mật

Các nguyên lí của ẩn mã

- Ẩn mã khóa công khai:
  - Sử dụng 2 khóa: khóa công khai (dùng trong quá trình nhúng) khóa riêng (trích xuất thông điệp)



Chương 2. Ẩn mã

An toàn và ẩn mã

- Mục đích truyền tin ẩn mã:
  - Che giấu sự tồn tại của thông báo bí mật
  - → Độ an toàn của một hệ ẩn mã được đánh giá bởi **khả năng không thể phát hiện** ra chứ không phải sự khó khăn trong việc đọc nội dung thông báo
- Bài toán phân tích ẩn mã là một bài toán quyết định:
  - Một đối tượng cho trước có chứa một thông điệp bí mật hay không
  - → Độ đo lí thuyết quyết định được coi là độ an toàn ẩn mã

An toàn và ẩn mã

- Trong phân tích ẩn mã, người ra quyết định có thể mắc hai loại sai lầm:
  - Không phát hiện
  - Phát hiện nhầm

An toàn và ẩn mã

- Kí hiệu:
  - β: Xác suất không phát hiện một đối tượng ẩn mã
  - α: Xác suất phát hiện nhầm một vật phủ là đối tượng ẩn mã (xác suất khẳng định sai – false positive probability)

An toàn và ẩn mã

Kết quả phân tích:

Thựctế / Kết quả phát hiện	**Vậtphủ**	**Vật ẩn mã**
Vật phủ	Từ chối đúng $1 - \alpha$	Không phát hiện β
Vậtẩnmã	Phát hiện nhầm α	Phát hiện đúng $1 - \beta$

An toàn và ẩn mã

- Theo lí thuyết thông tin, nếu độ đo an toàn của hệ ẩn mã là sự không phân biệt thống kê của các phân phối thì các xác suất sai lầm trên có thể được sử dụng trong khái niệm entropy tương đối nhị phân (binary relative entropy) $d(\alpha, \beta)$của hai phân phối nhị thức với các tham số $\alpha, 1-\alpha$và$1-\beta, \beta$

$$d(\alpha, \beta) = \alpha log \frac{\alpha}{1-\beta} + (1-\alpha) log \frac{1-\alpha}{\beta}$$

  - Nếu d(α, β) = 0 thì hệ ẩn mã đạt độ an toàn hoàn thiện và giá trị này càng lớn thì hệ ẩn mã càng dễ bị phát hiện

An toàn và ẩn mã

- Bằng trực quan con người đối với các sửa đổi ẩn mã cũng có thể được coi như một độ đo an toàn của ẩn mã
- Tuy nhiên, so với các phương pháp thống kê hiện đại thì hướng tiếp cận theo trực quan là ít tin cậy, phụ thuộc vào các đặc điểm hình ảnh cụ thể và không hoàn toàn tự động

An toàn và ẩn mã

- An toàn hoàn hảo:
  - Chọn vật phủ C với phân bố xác suất P_C
  - P_S là phân bố xác suất của $E_K(c, m, k)$ trên tập tất cả các vật có nhúng tin được sinh ra bởi hệ ẩn mã. $P_S(c) = 0$ nếu vật phủ c không bao giờ được sử dụng để nhúng tin

An toàn và ẩn mã

- Sử dụng định nghĩa entropy tương đối $D(P_C \| P_S)$giữa hai phân bố $P_C$và $P_S$trên tập C, ta có:

$$D(P_C \| P_S) = \sum_{c \in C} P_C(c) log \frac{P_C(c)}{P_S(c)}$$

đo độ không hiệu quả khi giả sử phân bố là $P_C$trong khi phân bố thực sự là P_S – tác động của quá trình nhúng tin trên phân bố $P_C$có thể đo được. Cụ thể, chúng ta định nghĩa độ an toàn của một hệ ẩn mã theo $D(P_C \| P_S)$.

An toàn và ẩn mã

- ***Địnhnghĩa 2.4*** *(Độ an toàn hoàn hảo).* Giả sử σ là một hệ ẩn mã, P_S là phân bố xác suất của các vật có nhúng tin gửi trên kênh, P_C là phân bố xác suất của C. σ được gọi là ε-an toàn đối với người tấn công thụ động nếu:

$$D(P_C \| P_S) \leq \varepsilon$$

Và gọi là an toàn hoàn hảo nếu $\varepsilon = 0$

- Do $D(P_C \| P_S) = 0$nếu và chỉ nếu hai phân bố là bằng nhau, chúng ta có thể kết luận rằng một hệ ẩn mã là an toàn hoàn hảo (về mặt lí thuyết), nếu như quá trình nhúng tin vào vật phủ không làm thay đổi phân bố xác suất củaC. Chúng ta có thể xây dựng một hệ ẩn mã với độ an toàn hoàn hảo.

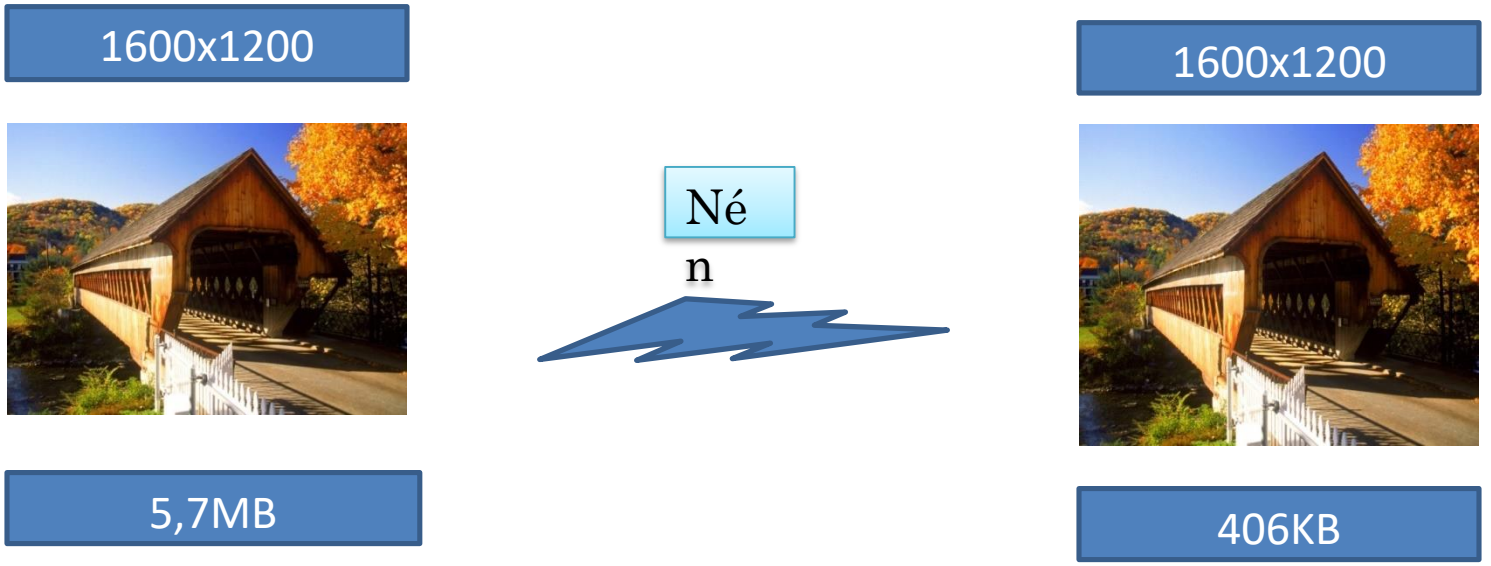
An toàn và ẩn mã

- ***Định lí 2.5*** Tồn tại hệ ẩn mã an toàn hoàn hảo.
- Chứng minh:
  - Giả sử C là tập các xâu bít có độ dài n. P_C là phân bố đều trên C, và e là một thông điệp mật ($e \in C$). Người gửi chọn ngẫu nhiên một $c \in C$ và tính $s = c \oplus e$, trong đó $\oplus$ là toán tử XOR bít. Vật có nhúng tin s sẽ được phân bố đều trên C, do vậy $P_C = P_S$ và $D(P_C \| P_S) = 0$. Trong quá trình trích xuất tin, thông điệp mật e có thể được xây dựng lại bằng cách tính $s \oplus c$.
  - Hệ thống trên rất đơn giản nhưng không hữu dụng, vì sẽ rất khó để Alice và Bob có thể trao đổi được các xâu bít ngẫu nhiên.

Chương 2. Ẩn mã

Các kĩ thuật trên ảnh số

- Xử lí ảnh: Nén JPEG
  - Thường giảm chất lượng màu nhưng không gây ra sự chú ý về chất lượng của hình ảnh



Hình ảnh được nén bằng thuật toán nén JPEG

Các kĩ thuật trên ảnh số

- Chuyểnđổiđiểmảnh sang YCbCr
  - $Y = 0.299R + 0.587G + 0.114B$
  - $U = 0.492(B - Y) = -0.147R - 0.289G + 0.436B$
  - $V = 0.877(R - Y) = 0.615R - 0.515G - 0.100B$
  - Mục đích:
    - Giảm giá trị thành phần màu
      - Mắt người thường nhạy cảm với những thay đổi về độ sáng hơn là những thay đổi về màu sắc $\Rightarrow$ giảm kích cỡ tổng thể của tệp thường sử dụng cách giảm chất lượng màu

Các kĩ thuật trên ảnh số

- Chuyển các giá trị điểm ảnh sang tần số:
  - Dùng biến đổi Fourier (DFT), Cosin rời rạc (DCT), …
  - DCT là tiêu chuẩn quốc tế cho các hệ thống mã chuyển vị
    - Vì có đặc tính gói năng lượng tốt, cho kết quả là số thực và có các thuật toán nhanh

Các kĩ thuật trên ảnh số

- DCT một chiều:
  - Quá trình biến đổi DCT thuận (FDCT) dung trong tiêu chuẩn JPEG được định nghĩa như sau:

$$X(k) = \sqrt{\frac{2}{N}} C(k) \sum_{m=0}^{N-1} x(m) \cos \frac{(2m+1)k}{\pi 2N}$$

  - Hàm biến đổi DCT ngược:

$$x(m) = \sqrt{\frac{2}{N}} \sum_{k=0}^{N-1} X(k) C(k) \cos \frac{(2m+1)k}{\pi 2N}$$

- Trongđó:
  - $X(k)$ là chuỗi kết quả
  - $x(m)$ là giá trị của mẫu m
  - k là chỉ số của hệ số khai triển
  - N là số mẫu có trong tín hiệu
  - $C(k) = \begin{cases} \frac{1}{\sqrt{2}} & nếu\ k = 0 \\ 1 & nếu\ k \neq 0 \end{cases}$

Các kĩ thuật trên ảnh số

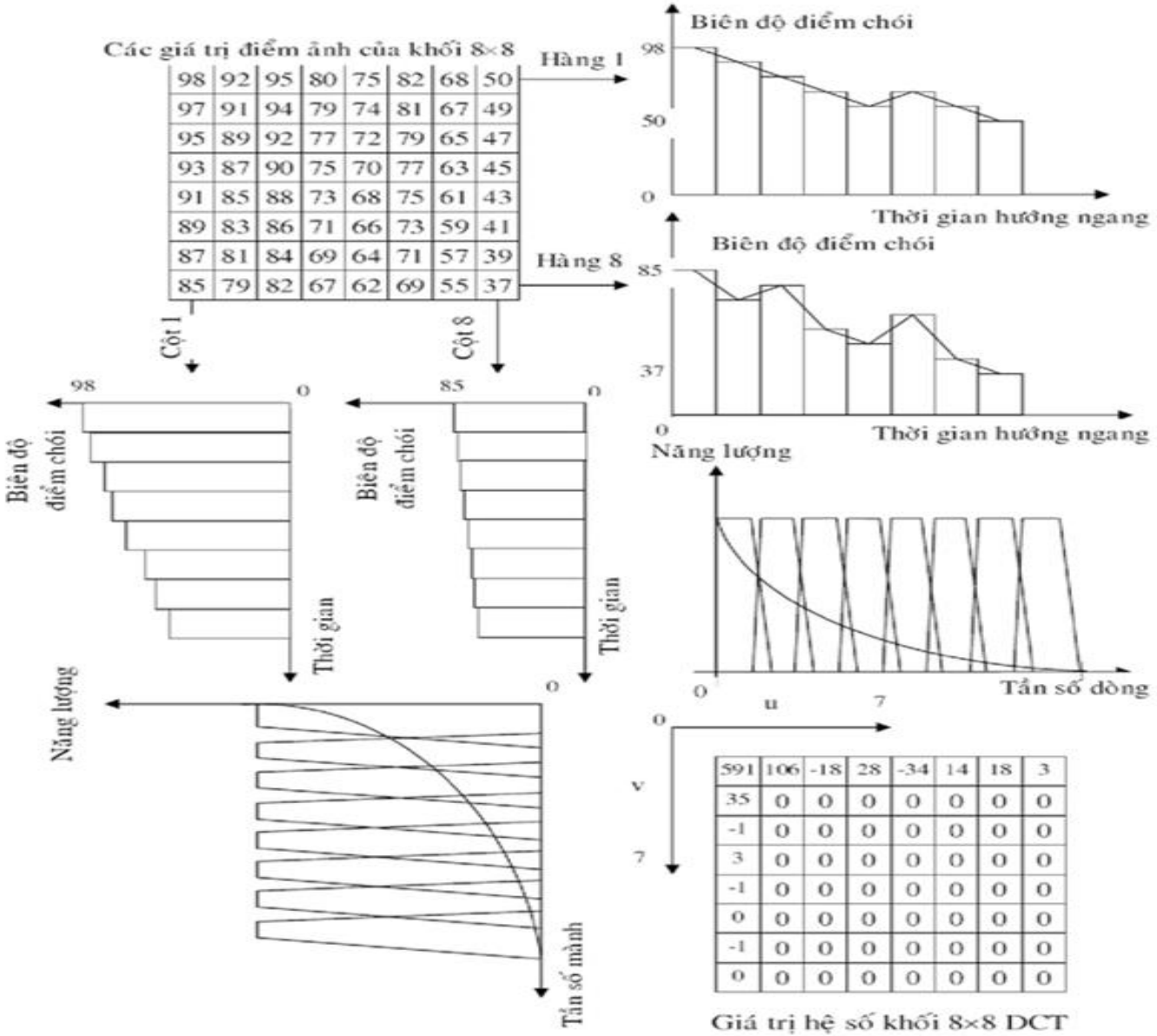
- DCT hai chiều:
  - Quá trình biến đổi DCT thuận:

$$F(u,v) = \frac{C(u)C(v)}{4}\sum_{j=0}^{7}\sum_{k=0}^{7} f(j,k)cos\frac{(2j+1)u\pi}{16}cos\frac{(2k+1)v\pi}{16}$$

  - Trong đó:
    - $f(j,k)$: các mẫu gốc trong khối điểm ảnh cỡ 8×8
    - u : Tần số chuẩn hóa theo chiều ngang $(0 < u < 7)$
    - v : Tần số chuẩn hóa theo chiều dọc$(0 < v < 7)$
    - $F(u,v)$: các hệ số biến đổi của khối DCT 8×8
    - $C(u), C(v) = \begin{cases} \frac{1}{\sqrt{2}} \; nếu\; u,v = 0 \\ 1 \quad nếu\; u,v \neq 0 \end{cases}$
  - Phép biến đổi DCT hai chiều là biến đổi đối xứng và biến đổi nghịch có thể tạo lại các giá trị mẫu $f(j,k)$ trên cơ sở các hệ số $F(u,v)$ theo công thức sau

$$f(j,k) = \sum_{j=0}^{7}\sum_{k=0}^{7} \frac{C(u)C(v)}{4}F(u,v)cos\frac{(2j+1)u\pi}{16}cos\frac{(2k+1)v\pi}{16}$$

Mã hóa khối 8 ×8 bằng DCT hai chiều



Các kĩ thuật trên ảnh số

- Lượng tử hóa
  - Là bước quan trọng nhất khi nén ảnh JPEG
  - Mục đích
    - Lượng tử các giá trị biểu thị cho hình ảnh sau giai đoạn chuyển đổi giá trị điểm ảnh sang tần số
  - Sau quá trình này một lượng lớn dữ liệu có thể được loại bỏ mà không ảnh hưởng tới chất lượng của ảnh

Các kĩ thuật trên ảnh số

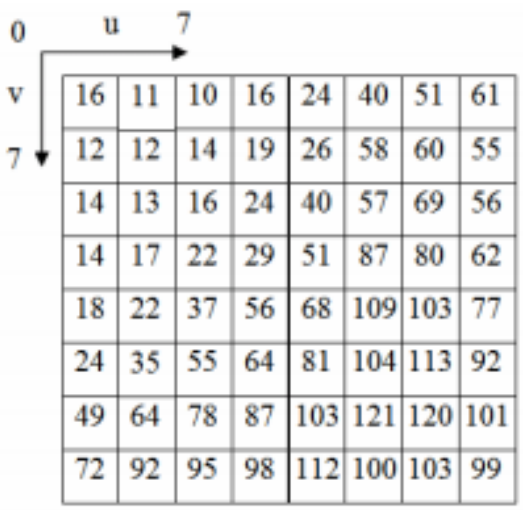
- Hệ số lượng tử hóa thuận được xác định theo biểu thức:

$$Fq(u,v) = round\left[\frac{F(u,v)}{Q(u,v)}\right]$$

- Quá trình lượng tử hóa có trọng số có xảy ra mất thông tin, gây tổn hao
  - Là bước tổn hao duy nhất trong thuật toán nén

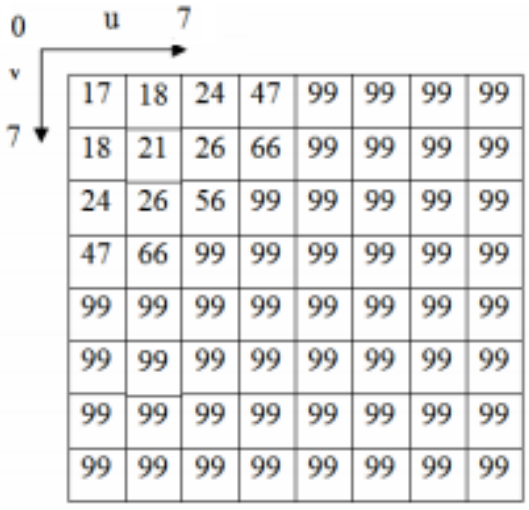
Các kĩ thuật trên ảnh số

- Việc biến đổi sao cho chất lượng hình ảnh do mắt người cảm nhận tốt, phụ thuộc vào các thành phần tần số và sự biến đổi chi tiết ảnh từng vùng trong miền không gian
  - Các ảnh càng chi tiết thì hệ số thành phần tần số cao càng lớn



16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Bảng trọng số (theo chuẩn JPEG cho mẫu tín hiệu chói)



17	18	24	47	99	99	99	99
18	21	26	66	99	99	99	99
24	26	56	99	99	99	99	99
47	66	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99

Bảng trọng số (theo chuẩn JPEG cho mẫu tín hiệu màu)

Các bảng lượng tử cho tín hiệu chói vào màu theo chuẩn JPEG

Các kĩ thuật trên ảnh số

- Khi nén ảnh theo JPEG, ma trận các hệ số khai triển sau DCT phải được nhân với bảng trọng số $Q(u,v)$ để loại bỏ một phần các hệ số có biên độ nhỏ (thường là các thành phần cao tần).

0 u 7

v

7

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Bảng trọng số (theo chuẩn JPEG cho mẫu tín hiệu chói)

0 u 7

v

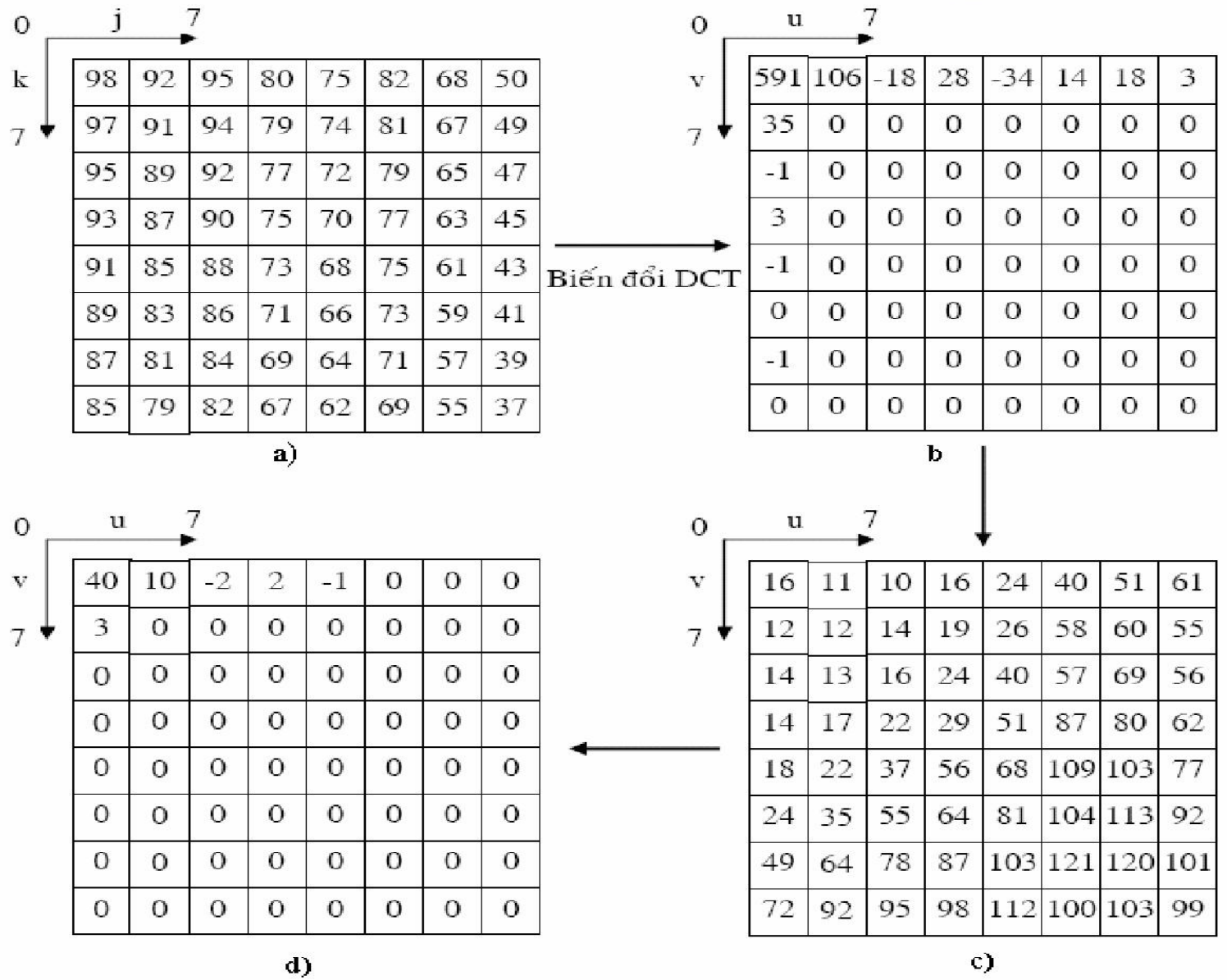
7

17	18	24	47	99	99	99	99
18	21	26	66	99	99	99	99
24	26	56	99	99	99	99	99
47	66	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99

Bảng trọng số (theo chuẩn JPEG cho mẫu tín hiệu màu)

Các bảng lượng tử cho tín hiệu chói vào màu theo chuẩn JPEG

Khai triển DCT và bảng trọng số Q(u,v)



- Ví dụ về quá trình biến đổi DCT một khối điểm ảnh có các giá trị điểm ảnh đen (giá trị = 0) và trắng (giá trị = 255) xen kẽ.

a) Khối 8x8 các điểm chói f(j,k)

k \ j	0	1	2	3	4	5	6	7
0	127	-128	127	-128	127	-128	127	-128
1	-128	127	-128	127	-128	127	-128	127
2	127	-128	127	-128	127	-128	127	-128
3	-128	127	-128	127	-128	127	-128	127
4	127	-128	127	-128	127	-128	127	-128
5	-128	127	-128	127	-128	127	-128	127
6	127	-128	127	-128	127	-128	127	-128
7	-128	127	-128	127	-128	127	-128	127

Biến đổi DCT

b) Khối các hệ số DCT tương ứng F(u,v)

v \ u	0	1	2	3	4	5	6	7
0	-5	0	0	0	0	0	0	0
1	0	33	0	39	0	58	0	166
2	0	0	0	0	0	0	0	0
3	0	39	0	46	0	69	0	196
4	0	0	0	0	0	0	0	0
5	0	58	0	69	0	103	0	294
6	0	0	0	0	0	0	0	0
7	0	166	0	196	0	294	0	837

d) Các hệ số DCT lượng tử hóa và chuẩn hóa $F_q(u,v)$

v \ u	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	3	0	2	0	1	0	3
2	0	0	0	0	0	0	0	0
3	0	2	0	2	0	1	0	3
4	0	0	0	0	0	0	0	0
5	0	1	0	1	0	1	0	3
6	0	0	0	0	0	0	0	0
7	0	3	0	3	0	3	0	8

c) Bảng trọng số Q(u,v)

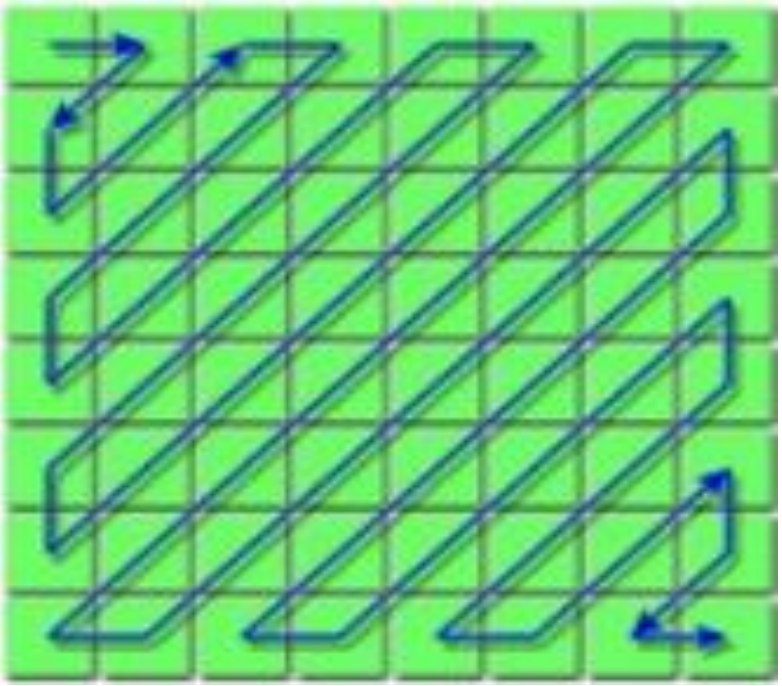
v \ u	0	1	2	3	4	5	6	7
0	16	11	10	16	24	40	51	61
1	12	12	14	19	26	58	60	55
2	14	13	16	24	40	57	69	56
3	14	17	22	29	51	87	80	62
4	18	22	37	56	68	109	103	77
5	24	35	55	64	81	104	113	92
6	49	64	78	87	103	121	120	101
7	72	92	95	98	112	100	103	99

Khai triển DCT cho khối ảnh có độ chói dạng bàn cờ

Các kĩ thuật trên ảnh số

- Sắp xếp zíc zắc:
  - Nhằm biến đổi mảng 2 chiều thành chuỗi số một chiều
    - VD: ma trận 8 × 8 sẽ thành véctơ 1 × 64
  - Sau khi lượng tử các hệ số DCT chỉ có một vài giá trị được giữ lại là khác 0 đa số sẽ luôn luôn là số 0
    - Các số khác 0 thường nằm ở phía bên trên bên trái và các số 0 ở góc dưới bên phải
  - Sắp xếp"zíc zắc" lại các hệ số trên để các tần số tương tự được nhóm lại với nhau

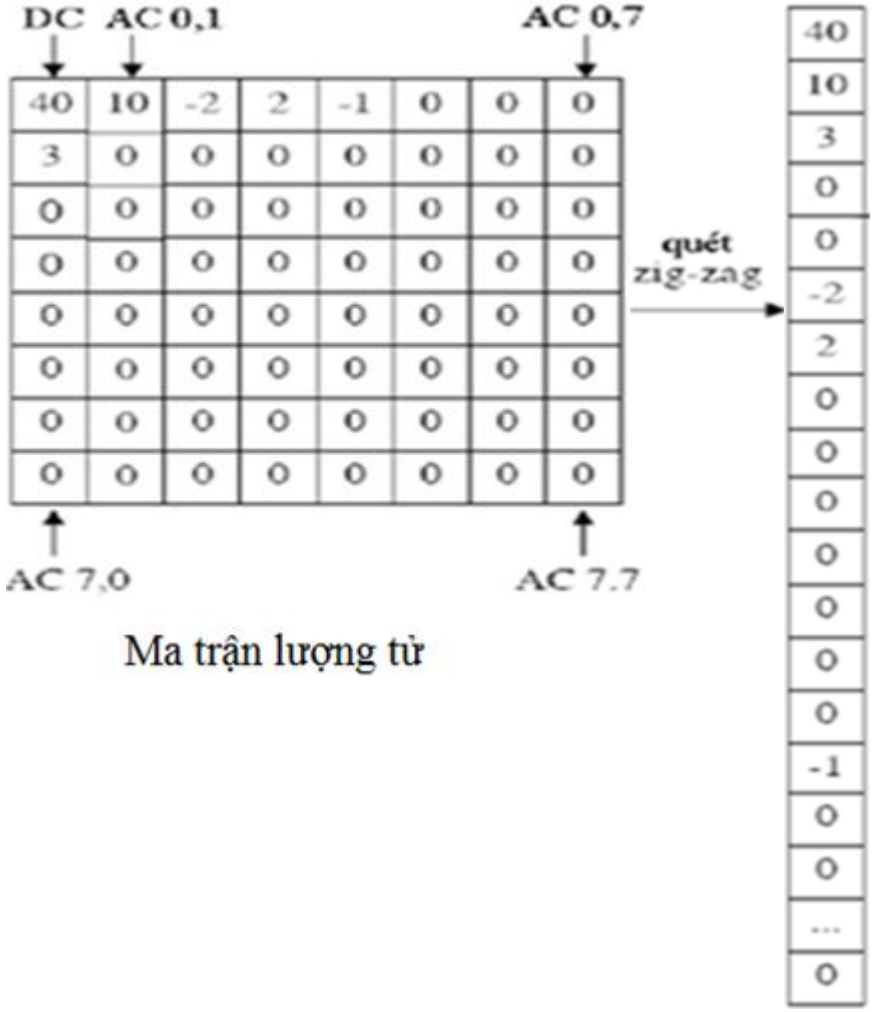
Các kĩ thuật trên ảnh số



Sắp xếp zíc zắc của các thành phần ảnh JPEG

Các kĩ thuật trên ảnh số

- VD: Quét Zíc zắc



Ma trận lượng tử

Các kĩ thuật trên ảnh số

- Mã hóa ước đoán (DPCM):
  - Dự đoán sự sai khác của hệ số DC so với khối trước (điều chế DPCM cho thành phần DC)
    - Do giá trị của DC là lớn, thay đổi nhưng gần với giá trị của khối trước đó
    - Giả sử đang thực hiện ở khối thứ i
      - Tính $\triangle = DC_i - DC_{i-1}$
      - VD: DC của khối hiện tại và khối trước lần lượt là 40 và 15 thì sử dụng mã DPCM sẽ được $\triangle = 40 - 15 = 25$

Các kĩ thuật trên ảnh số

- Mã hóa entropy, gồm:
  - Mã hóa RLC
  - Mã hóa VLC

Các kĩ thuật trên ảnh số

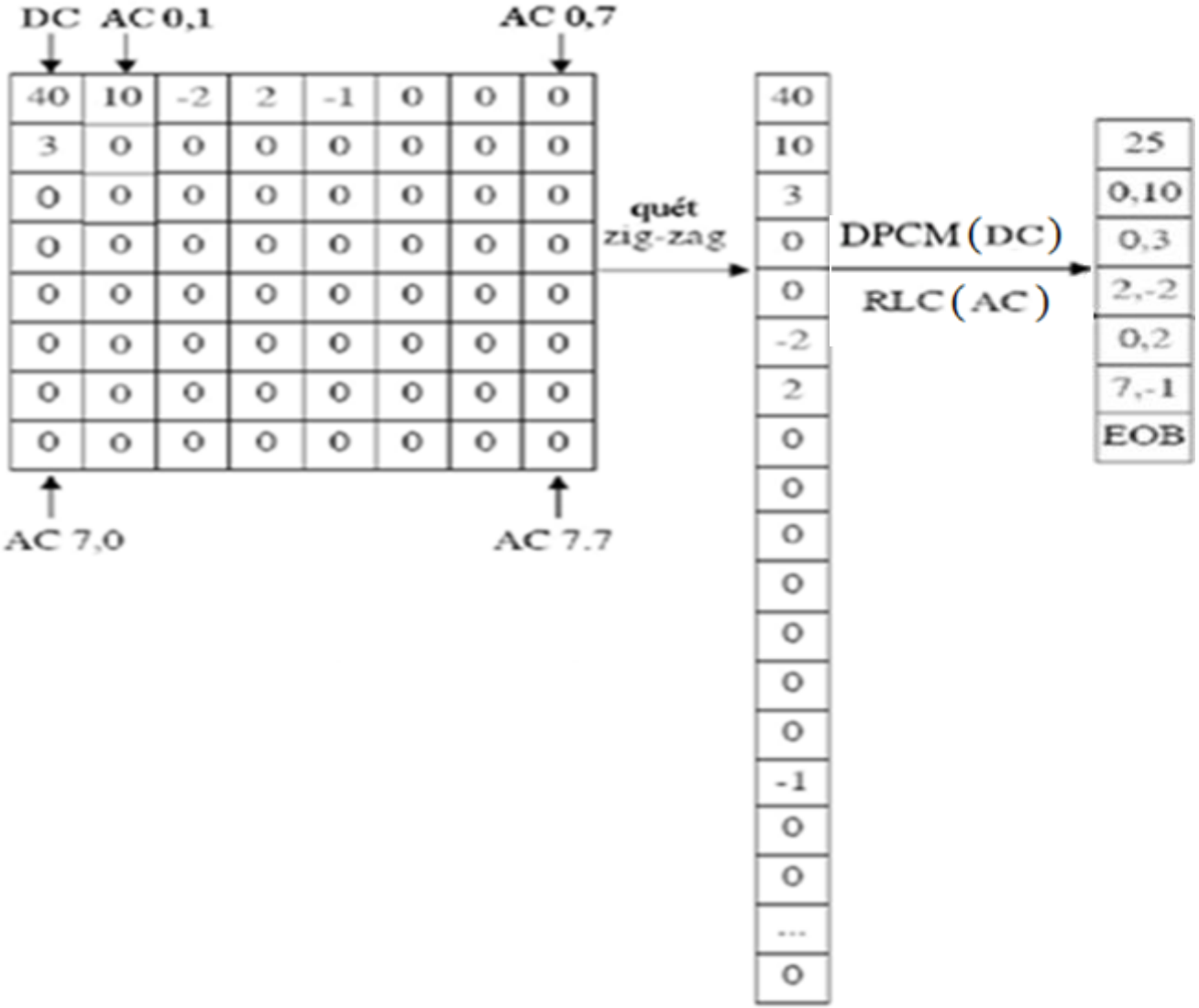
- Mã hóa loạt dài chạy (RLC):
  - Thành phần AC sau khi quét zíc-zắc thì các giá trị 0 giống nhau sẽ được thay bằng mã RLC
  - Dấu EOB: đánh dấu vị trí bắt đầu của chuỗi các số 0 liên tiếp
  - Nguyên tắc:
    - Bước 1: Phát hiện loạt (loạt giá trị giống nhau)
      - Cụ thể trong trường hợp này là loạt các giá trị 0 trước một giá trị khác 0
    - Bước 2: Kí hiệu mã
      - Thay loạt bằng một chuỗi mới gồm chiều dài của loạt (run length) và giá trị khác 0 tiếp theo
      - VD: có 5 giá trị 0 rồi tới giá trị 2 thì viết thành (5,2)

Các kĩ thuật trên ảnh số

- Mã hóa loạt dài chạy (RLC): (..)
  - Chỉ hiệu quả với chiều dài loạt lớn
    - Hiệu quả của việc mã hóa (nén) không cao
  - Để cải tiến hiệu quả dùng mã hóa entropy
    - Mã hóa entropy dùng những đặc tính thống kê của tín hiệu được mã hóa
    - Một tín hiệu, ở đây là giá trị điểm ảnh hoặc các hệ số chuyển vị, có chứa một lượng thông tin (entropy) tùy theo những xác suất của những giá trị hay sự kiện khác nhau xuất hiện
      - VD: những từ mã ít xảy ra hơn sẽ có nhiều thông tin hơn từ mã hay xảy ra

Các kĩ thuật trên ảnh số

- VD: Thực hiện mã DPCM và RLC



Các kĩ thuật trên ảnh số

- Mã hóa độ dài thay đổi (VLC)
  - Mã hóa thành phần DC: Giá trị hệ số sai lệch DC được mã hóa nhờ bảng phân loại và bảng Huffman
  - Mã hóa thành phần AC: Hệ số AC được mã hóa nhờ bảng phân loại (giống DC) và bảng Huffman (khác DC)

Các kĩ thuật trên ảnh số

- Bảng phân loại của DC và AC

Phạm vi	Loại DC	Loại AC
0	0	N/A
−1, 1	1	1
−3, −2, 2, 3	2	2
−7, . . . , −4, 4, . . . , 7	3	3
−15, . . . , −8, 8, . . . , 15	4	4
−31, . . . , −16, 16, . . . , 31	5	5
−63, . . . , −32, 32, . . . , 63	6	6
−127, . . . , −64, 64, . . . , 127	7	7
−255, . . . , −128, 128, . . . , 255	8	8
−511, . . . , −256, 256, . . . , 511	9	9
−1023, . . . , −512, 512, . . . , 1023	A	A
−2047, . . . , −1024, 1024, . . . , 2047	B	B

Các kĩ thuật trên ảnh số

- Bảng mã Huffman của DC

Phạm vi	Loại DC	Từ mã	Độ dài
0	0	010	3
−1, 1	1	011	4
−3, −2, 2, 3	2	100	5
−7, . . . , −4, 4, . . . , 7	3	00	5
−15, . . . , −8, 8, . . . , 15	4	101	7
−31, . . . , −16, 16, . . . , 31	5	110	8
−63, . . . , −32, 32, . . . , 63	6	1110	10
−127, . . . , −64, 64, . . . , 127	7	11110	12
−255, . . . , −128, 128, . . . , 255	8	111110	14
−511, . . . , −256, 256, . . . , 511	9	1111110	16
−1023, . . . , −512, 512, . . . , 1023	A	11111110	18
−2047, . . . , −1024, 1024, . . . , 2047	B	111111110	20

Bảng mã Huffman của AC

Loạt chạy/ Loại AC	Từ mã	Độ dài	Loạt chạy/ Loại AC	Từ mã	Độ dài
0/0	**1010 (= EOB)**	**4**			
0/1	00	3	8/1	11111010	9
0/2	01	4	8/2	1111111111000000	17
0/3	100	6	8/3	1111111110110111	19
0/4	1011	8	8/4	1111111110111000	20
0/5	11010	10	8/5	1111111110111001	21
0/6	111000	12	8/6	1111111110111010	22
0/7	1111000	14	8/7	1111111110111011	23
0/8	1111110110	18	8/8	1111111110111100	24
0/9	1111111110000010	25	8/9	1111111110111101	25
0/A	1111111110000011	26	8/A	1111111110111110	26
1/1	1100	5	9/1	111111000	10
1/2	111001	8	9/2	1111111110111111	18
1/3	1111001	10	9/3	1111111111000000	19
1/4	111110110	13	9/4	1111111111000001	20
1/5	11111110110	16	9/5	1111111111000010	21
1/6	1111111110000100	22	9/6	1111111111000011	22
1/7	1111111110000101	23	9/7	1111111111000100	23
1/8	1111111110000110	24	9/8	1111111111000101	24
1/9	1111111110000111	25	9/9	1111111111000110	25
1/A	1111111110001000	26	9/A	1111111111000111	26
2/1	11011	6	A/1	111111001	10
2/2	11111000	10	A/2	1111111111001000	18
2/3	1111110111	13	A/3	1111111111001001	19
2/4	1111111110001001	20	A/4	1111111111001010	20
2/5	1111111110001010	21	A/5	1111111111001011	21
2/6	1111111110001011	22	A/6	1111111111001100	22

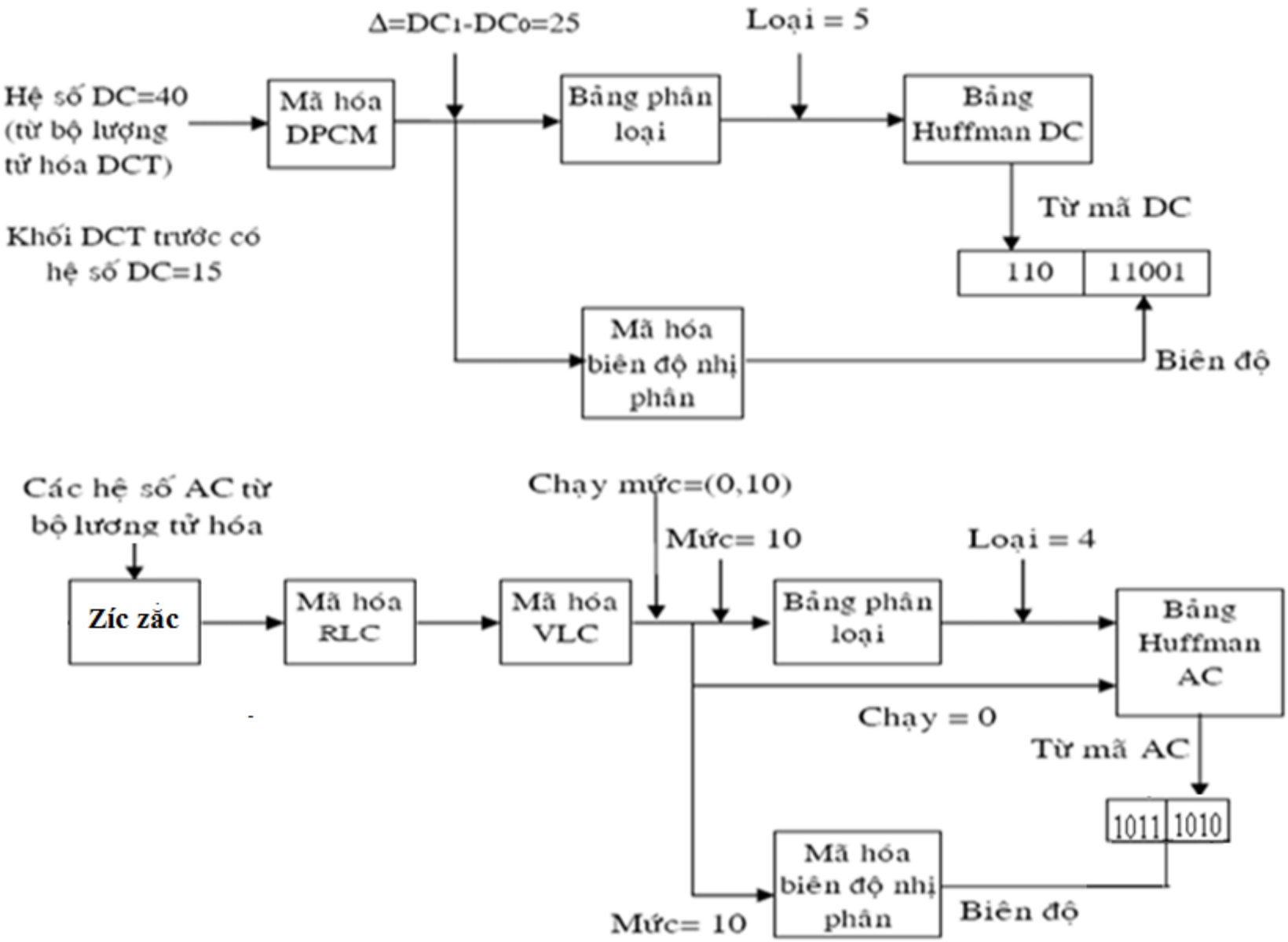
Các kĩ thuật trên ảnh số

- Chi tiết cách mã hóa DC:
  - Giá trị △ thu được sau điều chế DPCM được mã vào 2 phần, với độ dài mã
    - Phần 1: Mã ứng với loại của △
      - Từ bảng phân loại DC → loại của △
      - Từ bảng Huffman của DC → mã Huffman ứng với loại của △ và độ dài của từ mã ứng với giá trị △
      - VD: △=25 → thuộc loại 5 ứng với từ mã 110
    - Phần 2: Mã biên độ của △
      - Biên độ là vị trí của △ trong phạm vi mà nó thuộc vào (các vị trí được đánh số từ 0) (VD △=25 ứng với biên độ là 25)
      - Chuyển biên độ sang dạng nhị phân có độ dài bằng độ dài của từ mã ứng với △ trừ đi độ dài của mã phần 1
      - VD: △=25, có độ dài từ mã là 8, phần 1 có độ dài là 3 thì biên độ 25 sẽ được biểu diễn dưới dạng nhị phân có độ dài là 8-3=5, cụ thể mã là 11001 → Mã tổng thể của △=25 là 110 11001

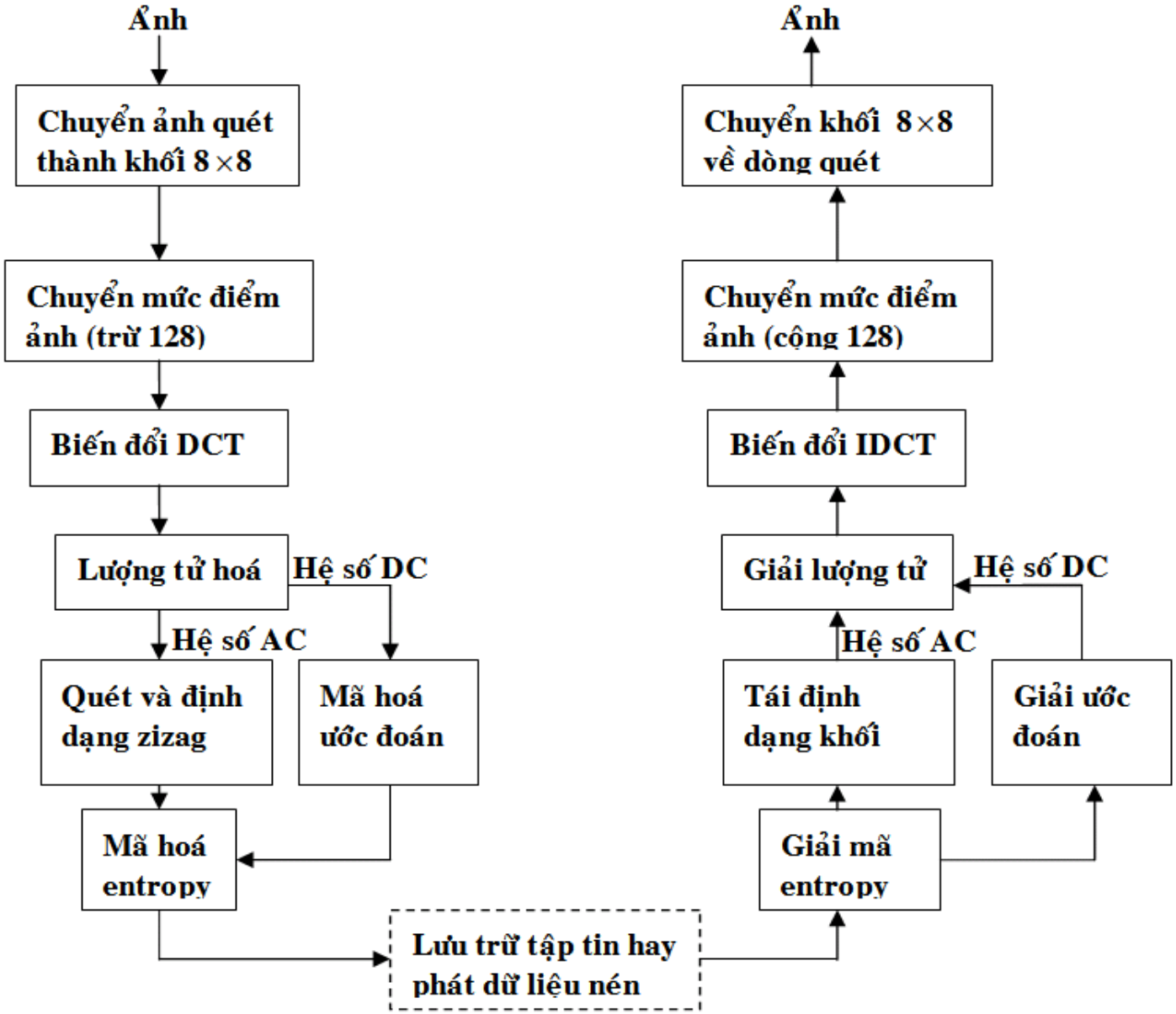
Các kĩ thuật trên ảnh số

- Chi tiết cách mã hóa AC:
  - Cũng mã thành 2 phần ứng với loại của AC và biên độ của giá trị AC tương tự đối với DC
  - VD: Mã RLC (0,10)
    - Từ bảng phân loại → Giá trị 10 thuộc loại 4 với biên độ là 10
    - Phần 1: mã tương ứng với (0,4) là 1011 (độ dài phần 1 là 4) và tổng độ dài mã giá trị AC là 8
    - Phần 2: chuyển biên độ 10 sang nhị phân với độ dài là 8-4=4, tức là 1010
    - → Mã VLC tổng thể của mã RLC (0,10) là 1011 1010

Sơ đồ khối hệ thống mã kết quả DCT sau khi lượng tử hóa

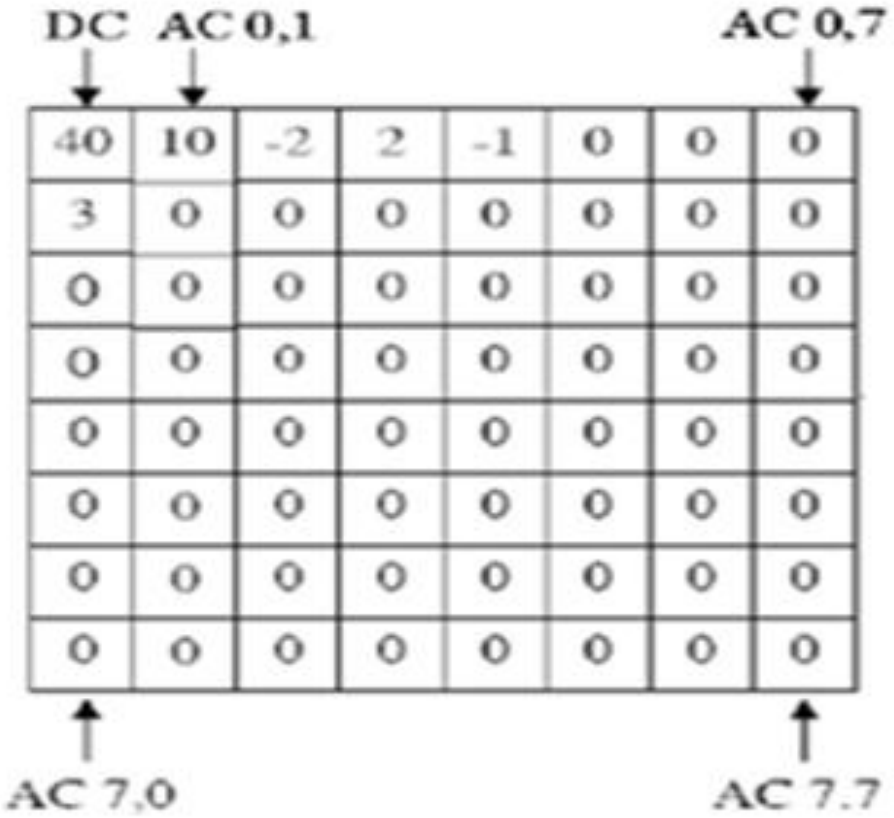


Mô hình chuẩn JPEG



Các kĩ thuật trên ảnh số

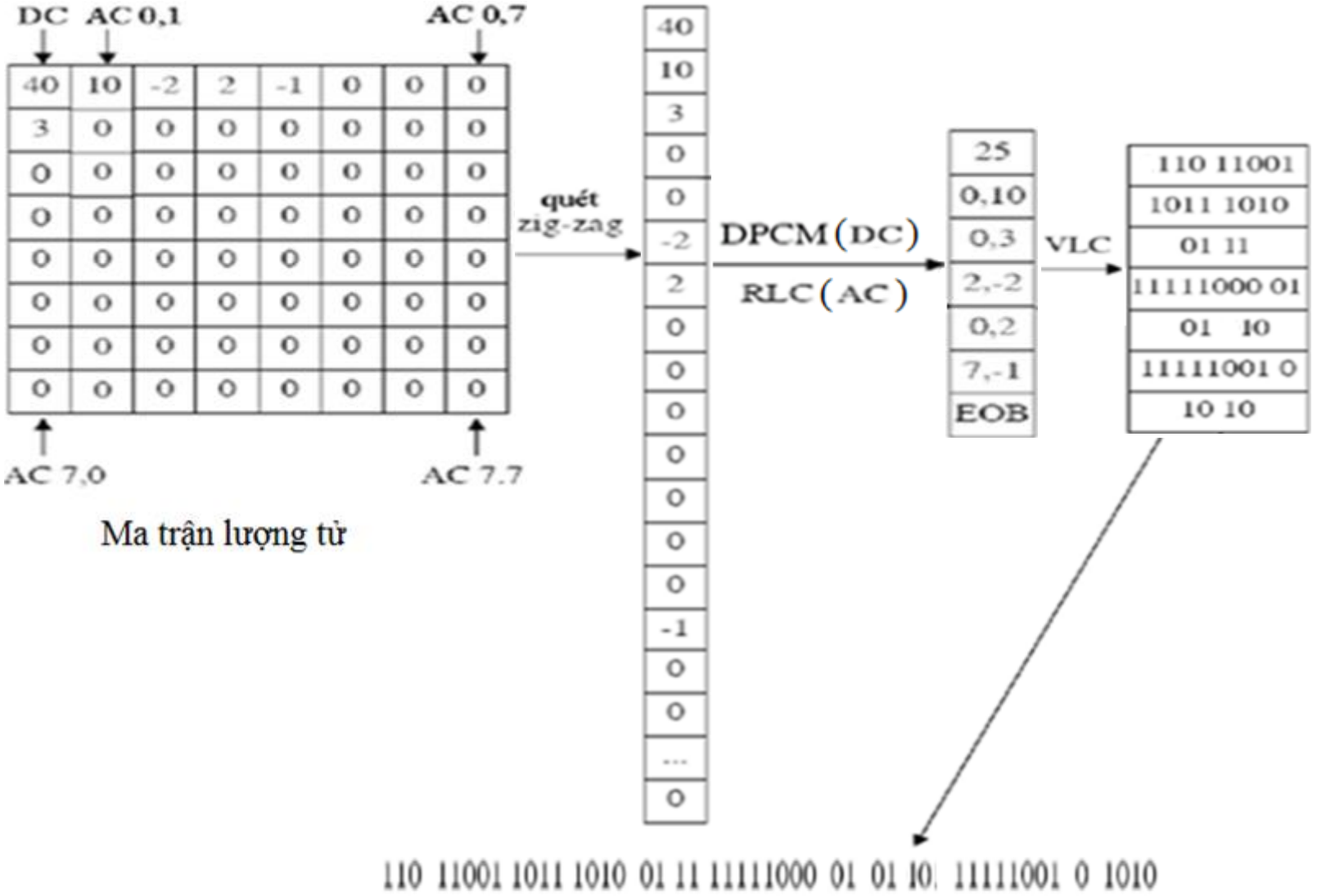
- VD: Cho ma trận ảnh lượng tử như sau, hãy mã hóa thành mã nhị phân biết giá trị DC của khối DCT trước là 15



40	10	-2	2	-1	0	0	0
3	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

Kết quả

- VD: Thực hiện mã DPCM và RLC



BT áp dụng

- Cho ma trận ảnh lượng tử:

$$\begin{bmatrix} 85 & -5 & -2 & 2 \\ 1 & 0 & 2 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

- Biết rằng hệ số DC của khối trước là 60. Hãy mã hóa ma trận ảnh thành mã nhị phân
- Kết quả: 11011001 100010 001 1111100001 0110 0110 000 1010

BT áp dụng

- Giải:

$$\begin{bmatrix} 85 & -5 & -2 & 2 \\ 1 & 0 & 2 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Zig zag →

85
-5
1
0
0
-2
2
2
-1
0
0
0
0
0
0
0

DPCM(DC)

RLC(AC) →

25
0, -5
0, 1
2, -2
0, 2
0, 2
0, -1
EOB

→

110 11001
100 010
001
11111000 01
01 10
01 10
00 0
1010

BTVN

- Sử dụng Matlab thực hiện tuần tự các bước chuyển mức điểm ảnh, biến đổi DCT, lượng tử hóa trong sơ đồ nén JPEG với MT đầu vào:

$$\begin{bmatrix} 52 & 55 & 61 & 66 & 70 & 61 & 64 & 73 \\ 63 & 59 & 55 & 90 & 109 & 85 & 69 & 72 \\ 62 & 59 & 68 & 113 & 144 & 104 & 66 & 73 \\ 63 & 58 & 71 & 122 & 154 & 106 & 70 & 69 \\ 67 & 61 & 68 & 104 & 126 & 88 & 68 & 70 \\ 79 & 65 & 60 & 70 & 77 & 68 & 58 & 75 \\ 85 & 71 & 64 & 59 & 55 & 61 & 65 & 83 \\ 87 & 79 & 69 & 68 & 65 & 76 & 78 & 94 \end{bmatrix}$$

- Ma trận lượng tử Q:

$$\begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix}$$

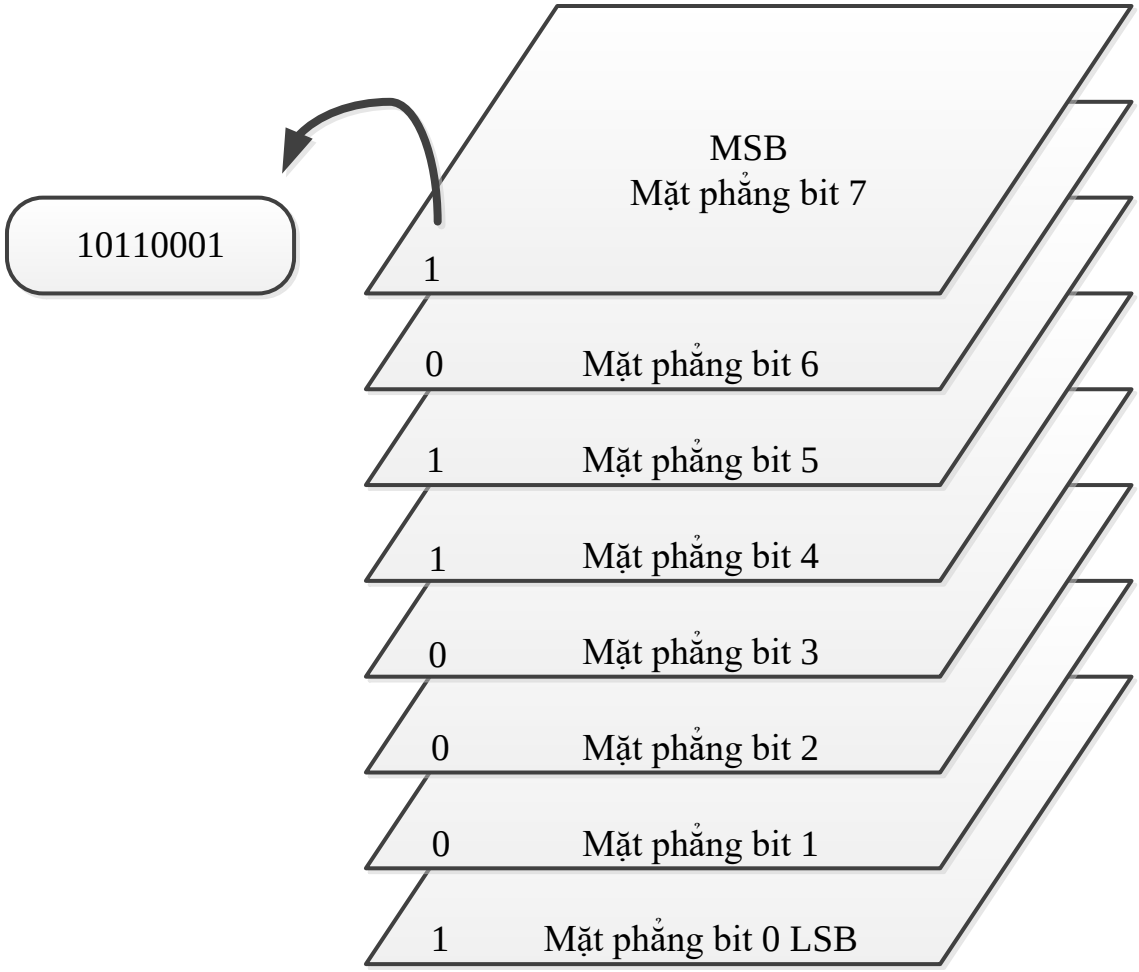
Các kĩ thuật trên ảnh số

- Kĩ thuật ẩn mã trên miền không gian ảnh
  - Kĩ thuật LSB
    - Tuần tự
    - Ngẫu nhiên
  - Kĩ thuật ẩn mã trong khối bít
- Kĩ thuật ẩn mã trên miền tần số
  - Jsteg
  - OutGuess 0.1
  - OutGuess 0.2
  - F3, F4, F5

Các kĩ thuật trên ảnh số

- Kĩ thuật LSB
  - KN: Bít có trọng số thấp nhất (LSB)
    - Là bít có ảnh hưởng ít nhất tới việc quyết định màu sắc của mỗi điểm ảnh
  - VD: Điểm ảnh biểu diễn bởi 8 bit 01110010**1**
    - 2 LSB: 0111001**01**
    - 3 LSB: 011100**101**

Các kĩ thuật trên ảnh số



Các mặt phẳng bít đối với biểu diễn dữ liệu 8 bit

Các kĩ thuật trên ảnh số

- Ví dụ minh họa: (Dùng Paint)
  - 1 điểm ảnh trên hệ màu RGB (15 – 128 – 10)

    0000 1111 – 1000 0000 – 0000 1010
  - Nếu thay bit LSB trên kênh B:

    0000 1111 – 1000 0000 – 0000 101**1**

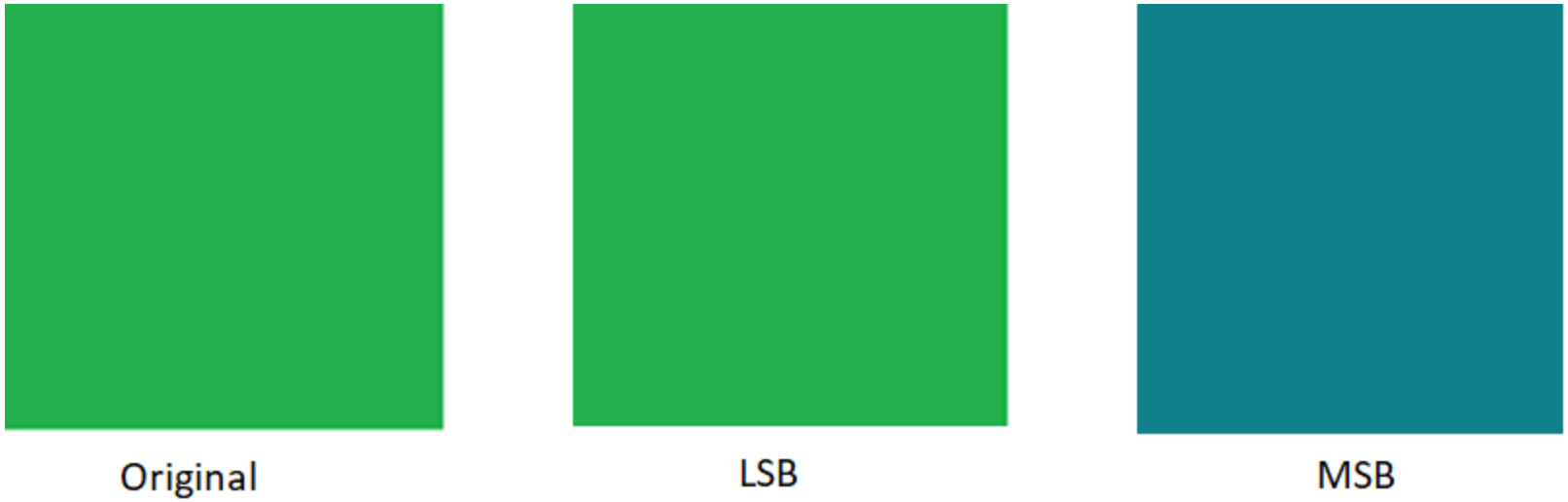
    (15 – 128 – 11)
  - Nếu thay bit MSB trên kênh B:

    0000 1111 – 1000 0000 – **1**000 1010

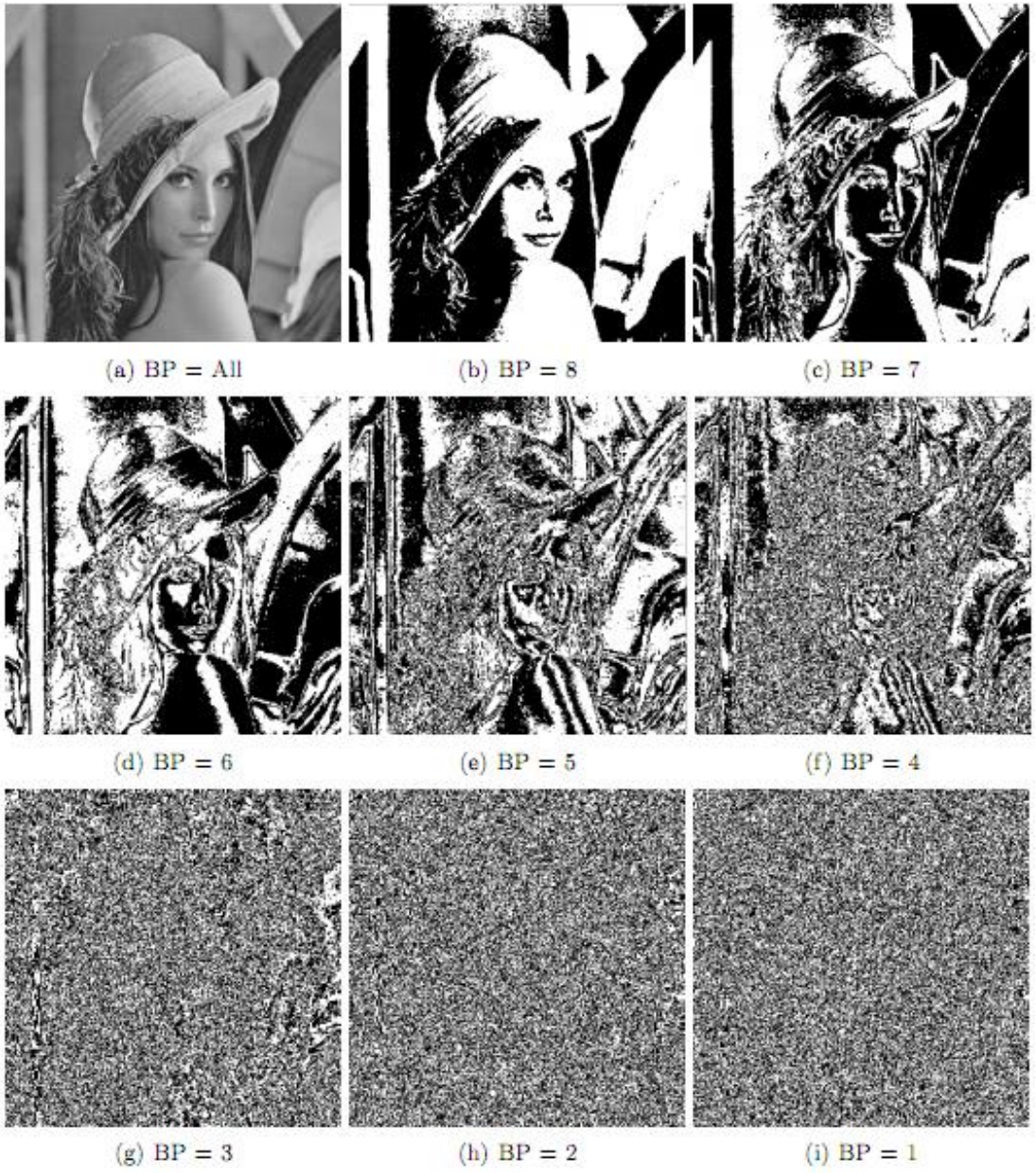
    (15 – 128 – 138)

Các kĩ thuật trên ảnh số

- Kĩ thuật LSB (..)
  - Kĩ thuật LSB là thay thế các bít có trọng số thấp nhất hay chèn thông tin cần giấu vào LSB



Các kĩ thuật trên ảnh số



Hình ảnh và các mặt phẳng bit giảm dần

Các kĩ thuật trên ảnh số

- Thuật toán giấu và tìm kiếm tuần tự:
  - Thuật toán nhúng:
    - *Đầu vào:* Ảnh phủ *c*, thông điệp *m*
    - *Đầu ra:* Ảnh có nhúng tin

1. for i = 1, ..., l(m) do
2. $p \leftarrow LSB(c_i)$
3. if $p \neq m_i$ then
4. $c_i \leftarrow m_i$
5. end if
6. end for

Các kĩ thuật trên ảnh số

- Thuật toán trích xuất:
  - *Đầu vào:* Ảnh có nhúng tin *s*
  - *Đầu ra:* thông điệp m'

1. for i = 1,...,l(s) do
2. $m'_i \leftarrow$ LSB(s_i)
3. end for

Các kĩ thuật trên ảnh số

- Thuật toán giấu và tìm kiếm ngẫu nhiên:
  - Thuật toán nhúng:
    - *Đầu vào:* Ảnh phủ *c*, khóa *k*, thông điệp *m*
    - *Đầu ra:* Ảnh có nhúng tin

1. Tạo vật ngẫu nhiên C từ dữ liệu c và mầm khóa k
   xáo trộn điểm ảnh
2. for i = 1,...,l(m) do
3. $p \leftarrow LSB(C_i)$
4. if $p \neq m_i$ then
5. $C_i \leftarrow m_i$
6. end if
7. end for
8. Trả về tạo độ gốc c từ dữ liệu C và mầm khóa k

Các kĩ thuật trên ảnh số

- Thuật toán trích xuất tin:
  - *Đầu vào:* Ảnh có nhúng tin s, khóa *k*
  - *Đầu ra:* Thông điệp m'

1. Tạo vật ngẫu nhiên S từ dữ liệu s và mầm khóa k

   xáo trộn điểm ảnh

2. for i = 1, ..., l(s) do

3. $m'_i \leftarrow \mathrm{LSB}(s_i)$

4. end for

Các kĩ thuật trên ảnh số

Bài tập áp dụng:

- Cho ma trận điểm ảnh của ảnh phủ C:

57	49	48	44	48	53
43	48	49	34	43	49
47	46	38	37	43	57
50	66	42	48	42	60
38	51	43	47	47	55
58	47	48	42	46	42

- Khóa k gồm các tham số (a, p) = (13 ,37). Xáo trộn các điểm ảnh của C theo công thức: $y_i = a^i \bmod p$. Với y_i là vị trí xáo trộn của điểm ảnh thứ i trong C
- Áp dụng thuật toán giấu và tìm kiếm ngẫu nhiên, em hãy nhúng thông điệp m = 0100111011 và trích xuất thông tin từ ma trận ảnh stego thu được

Các kĩ thuật trên ảnh số

- Kĩ thuật ẩn mã trong khối bít
  - Khá đơn giản
  - Thường áp dụng cho ảnh đen trắng (ảnh nhị phân)
  - Ý tưởng:
    - Chia ảnh thành các khối con cỡ $m \times n$
    - Giấu thông tin vào các khối con sao cho thỏa mãn một bất biến nào đó

Các kĩ thuật trên ảnh số

- Kĩ thuật ẩn mã trong khối bít (..)
  - Thuật toán Wu-Lee
    - Do M.Y.Wu và J.H.Lee đề xuất năm 1998
    - Chia ảnh nhị phân thành các khối đều nhau
    - Mỗi khối là một ma trận nhị phân
    - Giấu thông tin mật vào mỗi khối bằng cách thay đổi nhiều nhất một bít của khối

Các kĩ thuật trên ảnh số

- Thuật toán Wu-Lee (..)
  - Định nghĩa các phép toán AND ($\wedge$) và XOR ($\oplus$) hai bít *a*, *b* tùy ý

a	b	$a \wedge b$	$a \oplus b$
1	1	1	0
1	0	0	1
0	1	0	1
0	0	0	0

Các kĩ thuật trên ảnh số

- Thuật toánWu-Lee (..)
  - Định nghĩa các phép toán AND ($\wedge$) và XOR ($\oplus$) hai ma trận A và B bít cùng cấp
    - Nếu $A = (a_{ij}), B = (b_{ij}), C = (c_{ij}), D = (d_{ij})$
    - thì $A \wedge B = C$ với $c_{ij} = a_{ij} b_{ij}$
    - và $A \oplus B = D$ với $d_{ij} = a_{ij} \oplus b_{ij}$

Các kĩ thuật trên ảnh số

Thuật toán Wu-Lee (..)

VD phép AND và XOR hai ma trận bít

1	0	1	1
1	1	0	1
0	1	0	0
1	0	1	1

Ma trận A

0	0	1	0
0	1	1	1
1	0	1	0
1	1	0	1

Ma trận B

0	0	1	0
0	1	0	1
0	0	0	0
1	0	0	1

Ma trận C

1	0	0	1
1	0	1	0
1	1	1	0
0	1	1	0

Ma trận D

Các kĩ thuật trên ảnh số

- Thuật toánWu-Lee (..)
  - Định nghĩa: Cho X là một ma trận bít thì $SUM(X)$được xác định là tổng các giá trị 1 trên ma trận X
  - *VD: Xét hai ma trận A và B ở ví dụ trước*
    - *Thì* $SUM(A) = 10$
    - $SUM(B) = 9$

Các kĩ thuật trên ảnh số

- Thuật toánWu-Lee (..)
  - Thuật toán:
    - Đầu vào:
      - Ảnh gốc nhị phân F cỡ là bội của $m \times n$
      - Khóa bí mật K là một ma trận nhị phân cỡ $m \times n$
      - Thông điệp bí mật dưới dạng bít
    - Đầu ra: Ảnh F' có nhúng tin

Các kĩ thuật trên ảnh số

Thuật toán Wu-Lee (..)

Thuật toán: (..)

- Bước 1: Chia ảnh F thành các khối nhỏ, mỗi khối có kích thước là $m \times n$
- *Bước 2*: Với mỗi khối ảnh nhỏ F_i thu được từ bước 1, ta kiểm tra điều kiện sau:

$$0 < \boldsymbol{SUM}(\boldsymbol{F_i} \wedge \mathbf{K}) < \boldsymbol{SUM}(\boldsymbol{K})$$

  - Nếu đúng thì chuyển đến bước 3 để giấu thông tin vào trong khối F_i
  - Không đúng thì không giấu dữ liệu vào trong khối F_i (khối F_i được giữ nguyên)

Các kĩ thuật trên ảnh số

- Thuật toán Wu-Lee (..)
  - *Bước 3*: Gọi bít cần giấu vào trong khối F_i là b, thực hiện các bước sau để thay đổi F_i

if $(SUM(F_i \wedge K) \bmod 2 = b)$ **then** giữ nguyên F_i

else if $(SUM(F_i \wedge K) = 1)$ **then**

Chọn ngẫu nhiên một bít (j,k) thỏa mãn đồng thời

$[F_i]_{jk} = 0$ và $[K]_{jk} = 1$ sau đó chuyển giá trị của bít $[F_i]_{jk}$ thành 1

else if $(SUM(F_i \wedge K) = SUM(K) - 1)$ **then**

Chọn ngẫu nhiên một bít (j,k) thỏa mãn đồng thời

$[F_i]_{jk} = 1$ và $[K]_{jk} = 1$ sau đó chuyển giá trị của bít $[F_i]_{jk}$ thành 0

else Chọn ngẫu nhiên một bít mà $[K]_{jk} = 1$ chuyển giá trị của bít $[F_i]_{jk}$

từ 0 trở thành 1, hoặc từ 1 trở thành 0

Các kĩ thuật trên ảnh số

Thuật toán Wu-Lee (..)

VD:

- Cần nhúng thông tin B vào ảnh F sử dụng khóa K như sau

F_1			F_2		
1	1	0	1	1	1
1	1	1	1	1	0
0	1	0	0	0	0
0	0	1	0	0	0
1	1	0	1	1	1
0	1	1	0	1	0
F_3			F_4		

Thông tin giấu $B = 011$

1	1	0
1	1	1
0	1	0

K

Các kĩ thuật trên ảnh số

- Thuật toánWu-Lee (..)
  - Bước 1:
    - Chia ảnh F thành 4 khối nhỏ F_1, F_2, F_3, F_4 có kích thước là 3×3
  - Bước 2:
    - Với mỗi F_i, kiểm tra điều kiện$0 < SUM(F_i \wedge \mathrm{K}) < SUM(K)$
      - Đúng thì giấu vào F_i (thực hiện bước 3)
      - Sai thì giữ nguyên F_i (không giấu)

Các kĩ thuật trên ảnh số

Thuật toán Wu-Lee (..)

- Với F_1
  - Vì $0 < SUM(F_1 \wedge K) = SUM(K) = 6$ nên không giấu được dữ liệu vào trong F_1
- Với F_2
  - Vì $0 < SUM(F_2 \wedge K) = 4 < SUM(K) = 6$, nên một bít sẽ được giấu vào khối F_2 (giấu bit 0)
  - Thực hiện bước 3
    - Ta thấy $SUM(F_2 \wedge K)\ mod\ 2 = 4\ mod\ 2 = 0$ và cũng chính là bằng bít cần giấu $b = 0$ vì vậy khối F_2 được giữ nguyên

Các kĩ thuật trên ảnh số

Thuật toánWu-Lee (..)

Với F_3

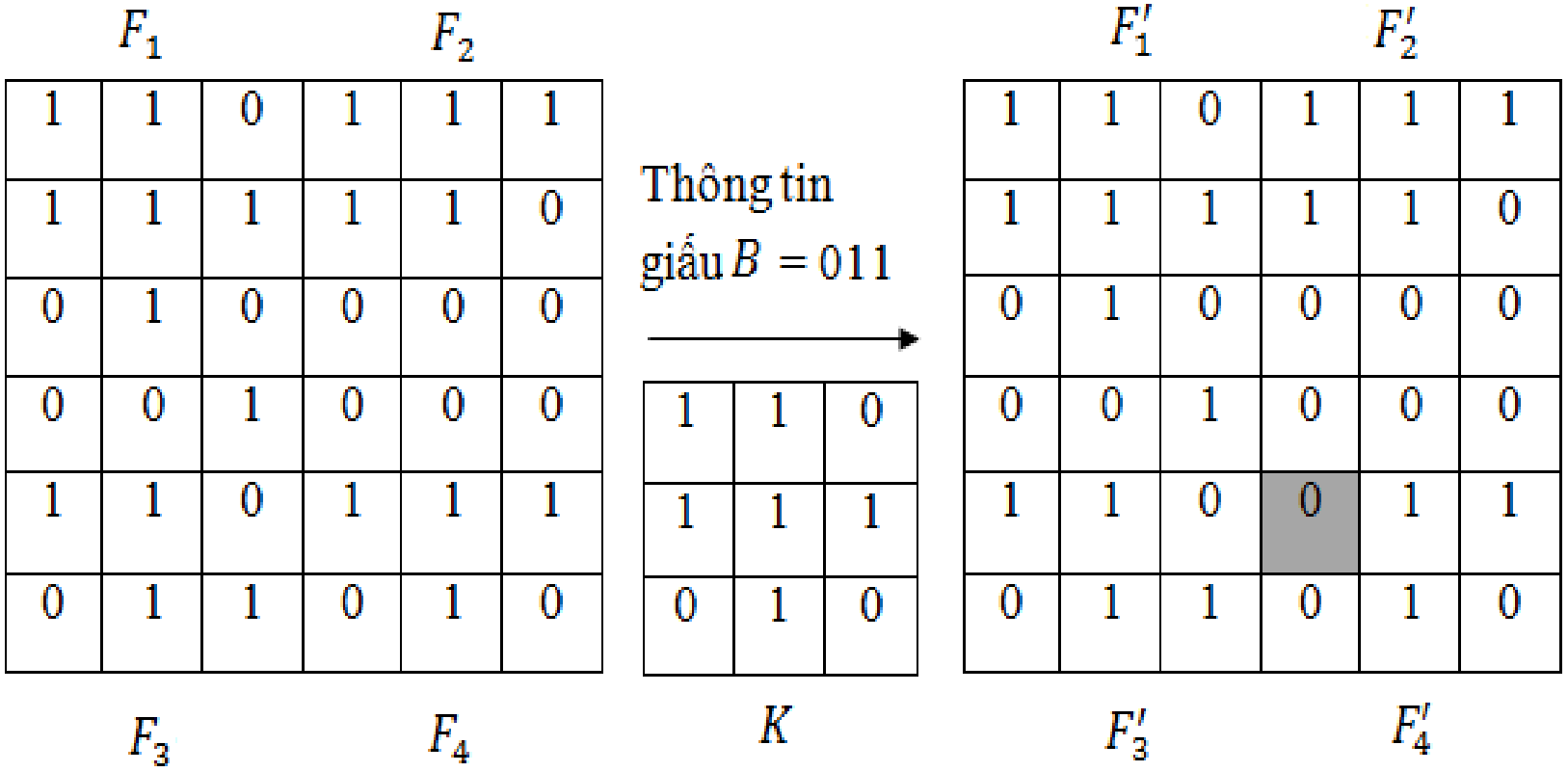
- Ta có $0 < SUM(F_3 \wedge K) = 3 < SUM(K) = 6$ nên có thể giấu bít thứ 2 là $b = 1$ vào khối này
- Thực hiện bước 3
  - Kiểm tra thấy $SUM(F_3 \wedge K)\ mod\ 2 = 3\ mod\ 2 = 1$ cũng chính bằng bít cần giấu nên ta vẫn giữ nguyên F_3

- Thuật toánWu-Lee (..)
  - VớiF_4
    - Ta có $0 < SUM(F_4 \wedge K) = 4 < SUM(K)$ nên có thể giấu bít thứ 3 là $b = 1$ vào khối này
    - Thực hiện bước 3
      - Kiểm tra thấy $SUM(F_4 \wedge K)\ mod\ 2 = 4\ mod\ 2 = 0 \neq b$
      - Kiểm tra $SUM(F_4 \wedge K) = 4 \neq 1\ v$à $\neq SUM(K) - 1 = 5$ vì vậy chọn ngẫu nhiên một bít $[K]_{jk} = 1$ rồi đảo bít $[F]_{jk}$, cụ thể ở đây ta chọn bít $[K]_{21} = 1$ và đảo bít $[F_4]_{21}$ từ 1 thành 0

Các kĩ thuật trên ảnh số

Thuật toán Wu-Lee (..)

Kết quả



Các kĩ thuật trên ảnh số

- ThuậttoánWu-Lee (..)
  - Nhận xét:
    - Khóa K nhằm làm tăng độ mật của thuật toán
      - Cần biết được kích thước khối là $m \times n$ và giá trị cụ thể của K
    - $F_i \wedge$K quy định thuật toán chỉ được phép sửa các bít trong khối F_i ứng với bít 1 trong khóa K
      - $\rightarrow$ K được xem như một mặt nạ, tạo ra khung nhìn cho thuật toán
      - Có thể thay phép $\wedge$ bằng các phép toán khác

Các kĩ thuật trên ảnh số

Thuật toán Wu-Lee (..)

Nhận xét: (..)

- Điều kiện $0 < SUM(F_i \wedge \mathrm{K}) < SUM(K)$
  - Loại trừ trường hợp $F_i \wedge$ K toàn 0 hoặc giống như khóa K thì không được giấu tin để tránh bị lộ
- Bước 3 tối đa chỉ đảo một bít của F_i
  - Để được khối F_i' thỏa mãn bất biến: $SUM(F_i' \wedge K)\ mod\ 2 = b$
  - Việc chọn bít trong F_i để đảo cần tuân theo nguyên tắc: Nếu $F_i \wedge$K có nhiều bít 1 thì chọn bít 1, ngược lại có quá ít bít 1 thì chọn bít 0
    - → Giảm khả năng bít đảo bị phát hiện

Các kĩ thuật trên ảnh số

Thuật toán Wu-Lee (..)

Nhận xét: (..)

- Trích xuất thông tin cần sử dụng bất biến này
  - Duyệt lần lượt các khối F_i' của ảnh đích F'. Nếu F_i' thỏa mãn điều kiện $0 < SUM(F_i' \wedge \mathrm{K}) < SUM(K)$ thì tính bít b đã được giấu vào trong khối bằng công thức tính $\boldsymbol{b = SUM(F_i \wedge K) \bmod 2}$
- Thay đổi nhiều nhất một bít của khối F_i khi giấu 1 bít thông tin vào trong khối nên với một khối có kích thước $m \times n$ đủ lớn thì sự thay đổi của F_i là nhỏ

Các kĩ thuật trên ảnh số

- Thuật toán Wu-Lee (..)
  - Nhận xét: (..)
    - Nên chọn ảnh *F* không được có quá nhiều điểm trắng hoặc có quá nhiều điểm đen
      - Vì tỉ lệ bít giấu được sẽ rất thấp
    - Nếu áp dụng đối với ảnh đen trắng, thuật toán chưa đạt được những yêu cầu cần thiết về dung lượng, độ an toàn cũng như chất lượng ảnh
      - Sử dụng ảnh màu thì kết quả khả quan hơn

Các kĩ thuật trên ảnh số

Bài tập:

- Áp dụng thuật toán giấu tin trong khối bit Wu – Lee thực hiện nhúng và trích xuất tin B = 010 vào ảnh F sử dụng khóa K, với các giả thiết cho ở dưới.

Ảnh F

1	1	0	1	0	1
1	0	1	1	1	1
0	1	1	0	1	0
0	1	0	1	1	1
1	1	1	0	0	0
0	1	1	1	0	0

Khóa K

0	1	0
1	1	1
0	1	1

- Với một khối ảnh con nào đó, tại sao trong trường hợp $sum(F_i \wedge K) = 1$ thì phải chọn vị trí điểm ảnh có bit bằng 0 để đảo?
- Bất biến của thuật toán này là gì? Vai trò của bất biến đó thể hiện như thế nào?

Các kĩ thuật trên ảnh số

- Kĩ thuật ẩn mã trên miền tần số (DCT, DFT)
  - Sử dụng phương pháp biến đổi trực giao chẳng hạn như Cosine rời rạc hay Fourier,… để chuyển miền không gian ảnh sang miền tần số.
  - Thông điệp sẽ được nhúng trong miền không gian tần số của ảnh theo kĩ thuật trải phổ trong truyền thông.

Các kĩ thuật trên ảnh số

Thuật toán Jsteg

Quá trình nhúng tin:

- *Đầu vào:* Ảnh phủ *c*, thông điệp *m*
- *Đầu ra:* Ảnh có nhúng tin *s*

1. Chuyển đổi ảnh *c* sang miền DCT *d* trong các khối 8×8
2. for i=1,...,l(m) do
3. p ← hệ số DCT tiếp theo từ d
4. while p=DC or p=0 or p=1 do
5. p ← hệ số DCT tiếp theo từ d
6. end while
7. $p_i \leftarrow p \bmod 2 + m_i$
8. $d_i \leftarrow p_i$
9. end for
10. Chuyển đổi mỗi khối 8×8 trở lại miền không gian để được *s*

Các kĩ thuật trên ảnh số

- Quản lí trích xuất tin:
  - *Đầu vào:* Ảnh phủ *c*, thông điệp *m*
  - *Đầu ra:* Ảnh có nhúng tin *s*

1. Chuyển đổi ảnh *s* sang miền DCT d trong các khối 8×8
2. for i=1,...,l(s) do
3. p ← hệ số DCT tiếp theo từ d
4. while p=DC or p=0 or p=1 do
5. p ← hệ số DCT tiếp theo từ d
6. end while
7. $m_i \leftarrow p \bmod 2$
8. end for

Các kĩ thuật trên ảnh số

Bài tập áp dụng:

- Cho ma trận các hệ số DCT 8 × 8 như sau:

1480	49	-61	0	0	0	1	0
10	0	1	-22	11	8	0	0
1	1	0	0	0	0	0	0
-19	0	1	27	1	1	1	1
1	1	0	0	0	0	0	0
-30	0	-19	1	0	1	0	1
0	0	0	0	1	-4	1	0
1	1	0	0	1	0	1	1

- Áp dụng thuật toán Jsteg để ẩn đoạn mã 8 bit m = 00101101 và thực hiện trích xuất m sau khi nhúng.

Thuật toán OutGuess 0.1:

□ Quá trình nhúng tin:

- *Đầu vào:* Ảnh phủ *c*, thông điệp *m*, khóa *k*
- *Đầu ra:* Ảnh có nhúng tin

1. Chuyển đổi ảnh c sang miền DCT d trong các khối 8×8
2. Tạo chuỗi giả ngẫu nhiên dùng dữ liệu d và khóa k
3. for i=1,...,l(m) do
4. p ← hệ số giả ngẫu nhiên DCT tiếp theo của ảnh c
5. while p=DC or p=0 or p=1 do
6. p ← hệ số giả ngẫu nhiên DCT tiếp theo của ảnh
7. end while
8. $p_i \leftarrow p \bmod 2 + m_i$
9. $c_i \leftarrow p_i$
10. end for
11. Đưa các hệ số đã xáo trộn trở về vị trí ban đầu (dùng mầm khóa k)
12. Chuyển đổi mỗi khối 8×8 trở lại miền không gian

Quá trình xuất tin:

- *Đầu vào:* Ảnh có nhúng tin *s*
- *Đầu ra:* Thông điệp *m*

1. Chuyển đổi ảnh s sang miền DCT *d* trong các khối 8×8
2. Tạo chuỗi giả ngẫu nhiên dùng dữ liệu *d* và khóa *k*
3. for i=1,...,l(s) do
4. p ← hệ số giả ngẫu nhiên DCT tiếp theo của ảnh s
5. while p=DC or p=0 or p=1 do
6. p ← hệ số giả ngẫu nhiên DCT tiếp theo của ảnh
7. end while
8. m_i ← p mod 2
9. end for

Các kĩ thuật trên ảnh số

- Bài tập áp dụng:
  - Cho ma trận các hệ số DCT 8 × 8 như sau:

1480	49	-61	0	0	0	1	0
10	0	1	-22	11	8	0	0
1	1	0	0	0	0	0	0
-19	0	1	27	1	1	1	1
1	1	0	0	0	0	0	0
-30	0	-19	1	0	1	0	1
0	0	0	0	1	-4	1	0
1	1	0	0	1	0	1	1

  - Dựa trên thuật toán Outguess, yêu cầu:
    - Tạo chuỗi giả ngẫu nhiên DCT bằng cách trích rút các hệ số DCT trên theo sắp xếp zig – zag, sau đó dịch phải k = 3 vị trí
    - Thực hiện ẩn tin m = 01101011 trong khối ma trận trên

Các kĩ thuật trên ảnh số

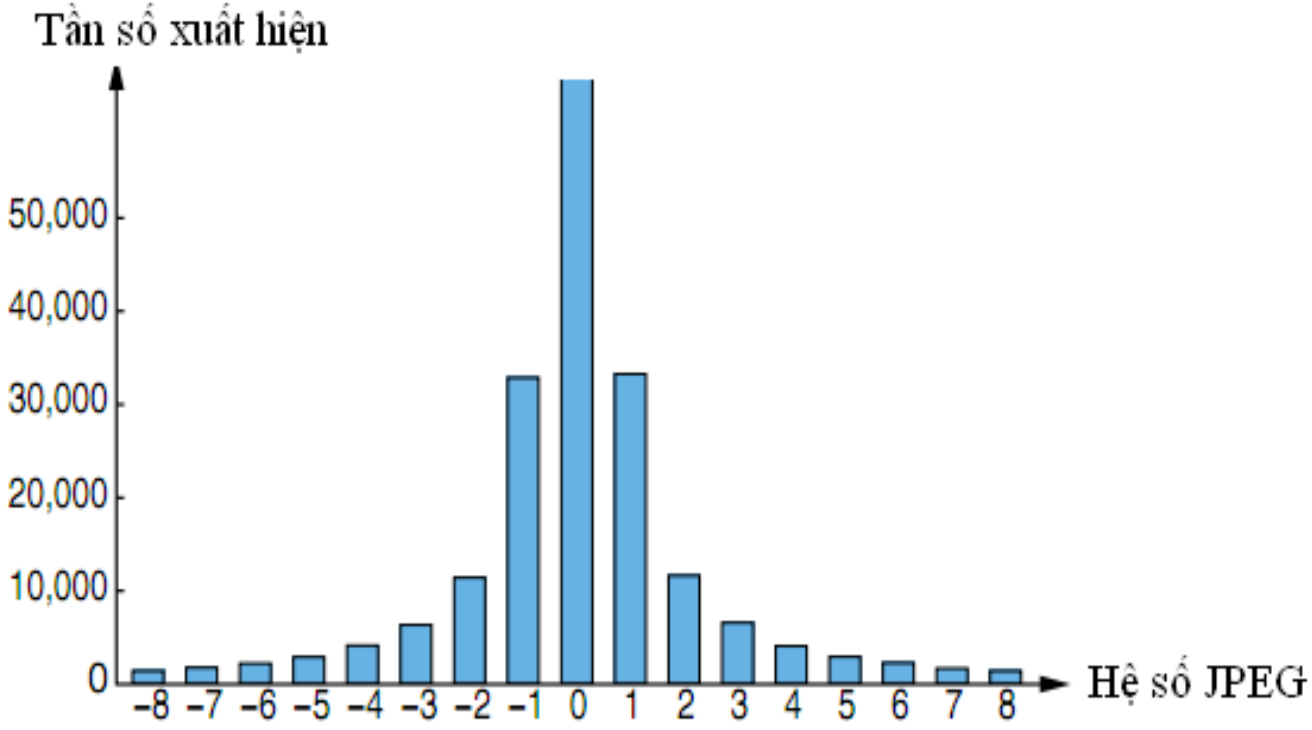
- Thuật toán Outguess 0.2:
  - Tương tự như Outguess 0.1, tuy nhiên sau khi nhúng tin có thêm quá trình hiệu chỉnh để ảnh sau khi nhúng có đặc tính tương tự như một hình "ảnh sạch" giúp chống lại được phương pháp phân tích thống kê

Các kĩ thuật trên ảnh số

- Thuật toán F3:
  - Không ghi đè các bit mà giảm giá trị tuyệt đối của hệ số được nhúng. Không sử dụng hệ số 0 để nhúng
  - LSB của hệ số khác 0 giống với thông điệp mật sau khi nhúng thì không ghi đè các bit vì kiểm tra khi bình phương có thể dễ dàng phát hiện ra những thay đổi đó.
  - Trái ngược với Jsteg, F3 sử dụng các hệ số có giá trị 1.

Các kĩ thuật trên ảnh số

- Đối xứng của 1 và -1 có thể thấy trong hình dưới đây

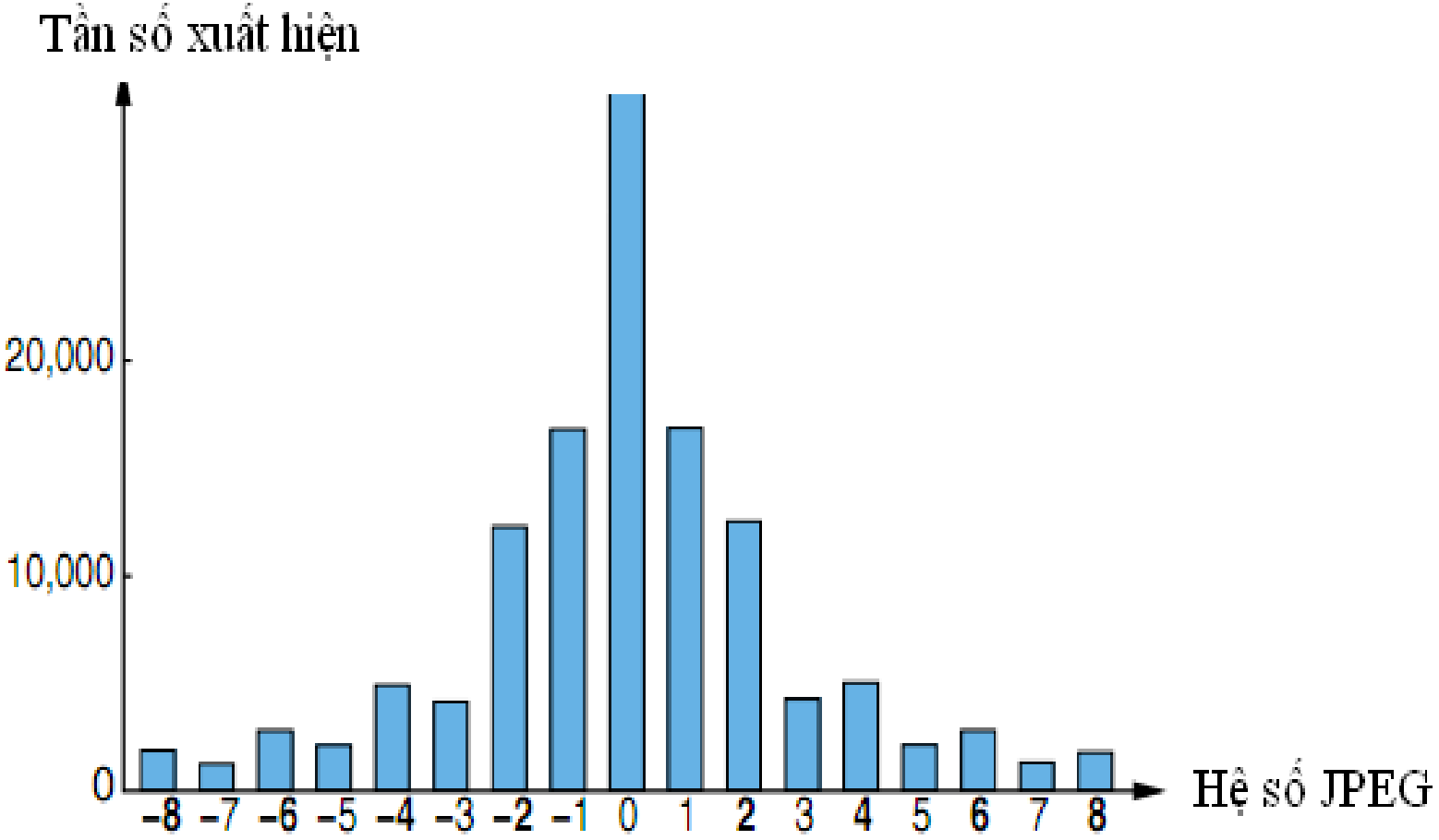


Biểu đồ các hệ số JPEG sau khi lượng tử hóa

Các kĩ thuật trên ảnh số

- Một số bít được nhúng có thể gây nên sự hao hụt trong trường hợp thuật toán F3 giảm giá trị tuyệt đối của 1 và -1 thành 0. Người nhận không thể phân biệt được đâu là hệ số 0 thực sự hay là được sinh ra từ sự hao hụt trên.
- Thuật toán trích xuất sẽ bỏ qua tất cả các hệ số bằng 0. Do đó, người gửi sẽ nhúng lại các bít bị ảnh hưởng khi chính họ tạo ra hệ số 0.

Các kĩ thuật trên ảnh số

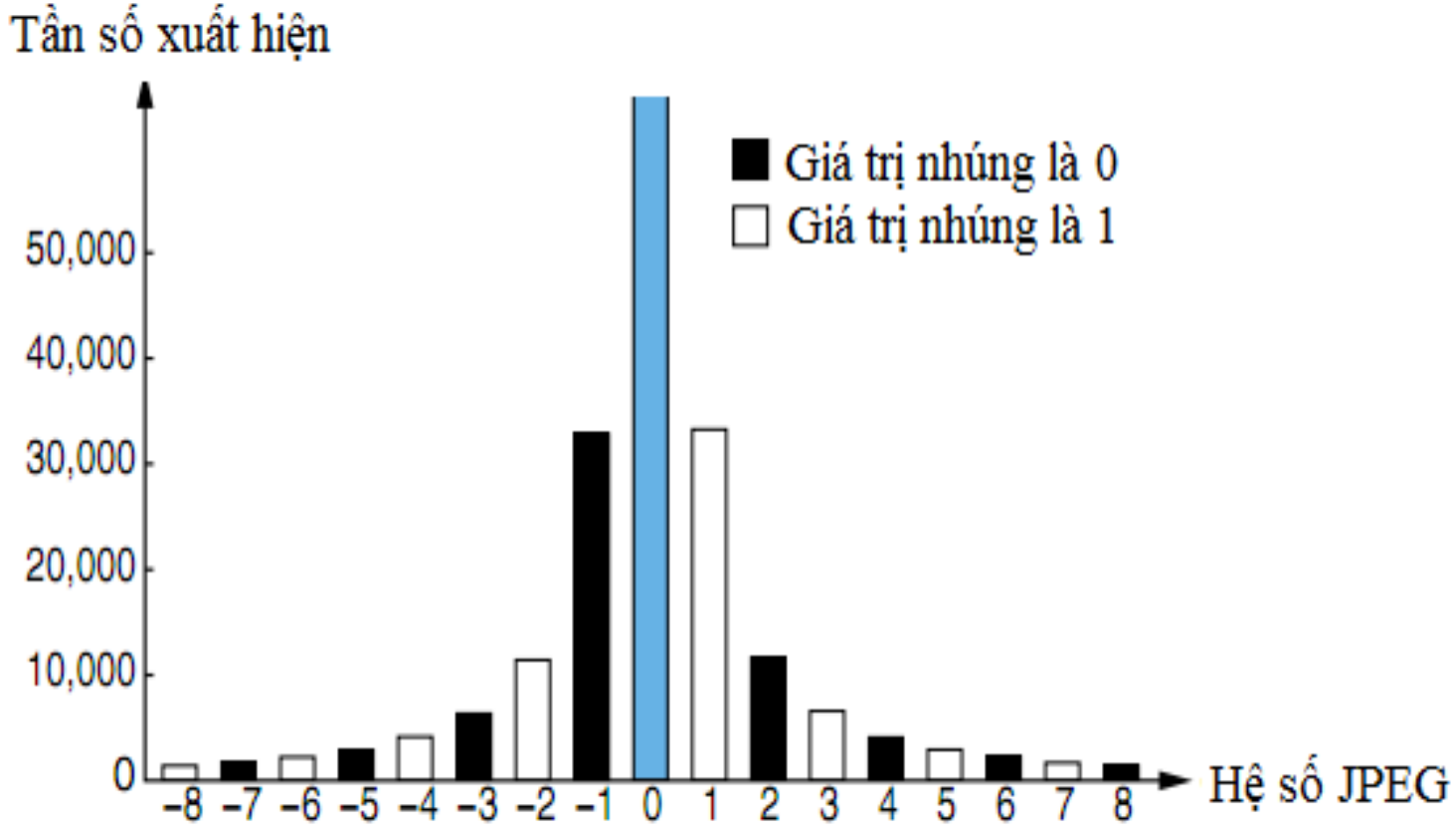


F3 tạo ra một số lượng lớn các hệ số chẵn

Các kĩ thuật trên ảnh số

- Thuật toán F4: loại bỏ 2 điểm yếu của F3 (sự hao hụt, nhiều hệ số chẵn hơn so với hệ số lẻ) bằng cách ánh xạ các hệ số âm thành các giá trị ẩn mã ngược:
  - Các hệ số chẵn âm biểu diễn cho giá trị ẩn mã 1, lẻ âm là 0, chẵn dương biểu diễn cho 0, lẻ dương cho 1
    - Ví dụ: Nhúng 0 vào một hệ số DCT bằng -3, kết quả sẽ vẫn là -3, trong khi nếu dùng F3 thì nó sẽ được thay bằng -2

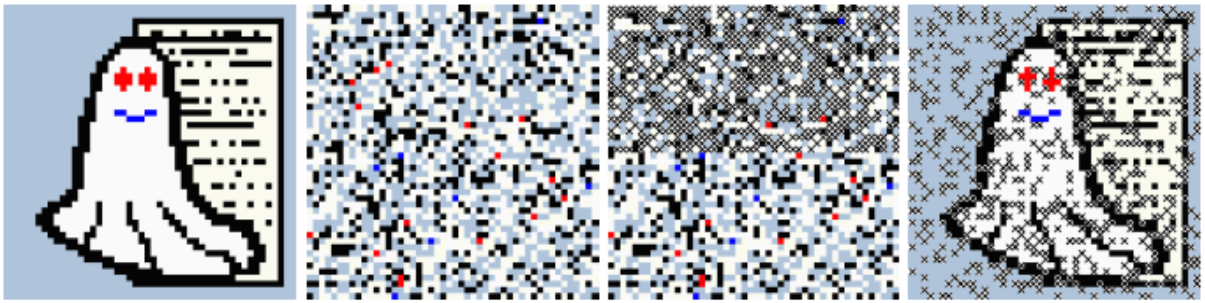
Các kĩ thuật trên ảnh số



Biểu đồ các hệ số JPEG với thuật toán F4

Các kĩ thuật trên ảnh số

- Thuật toán F5:
  - Sắp xếp hoán vị:
    - F5 sử dụng hoán vị để sắp xếp lại các hệ số trước rồi sau đó thực hiện nhúng tuần tự
    - Phép hoán vị phụ thuộc vào một khóa được lấy từ mật khẩu



Phép nhúng hoán vị phân phối những sự thay đổi(×)

Các kĩ thuật trên ảnh số

- Ma trận nhúng:
  - Ví dụ:
    - Nhúng một thông điệp rất ngắn chỉ 217 byte (1736 bít), thuật toán F4 thay đổi 1157 vị trí trong ảnh Expro ở hình sau.
    - Tuy nhiên, thuật toán F5 cũng nhúng thông điệp đó bằng cách sử dụng ma trận nhúng chỉ thay đổi 459 vị trí.

Các kĩ thuật trên ảnh số

- Quá trình nhúng được mô tả:
  - Nhúng hai bit x_1, $x_2$vào 3 bit có thể sửa là a_1, a_2, $a_3$mà chỉ thay đổi nhiều nhất là 1 bit. Có 4 trường hợp có thể xảy ra:
    - $x_1 = a_1 \oplus a_3, x_2 = a_2 \oplus a_3 \Longrightarrow$ không cần thay đổi gì
    - $x_1 \neq a_1 \oplus a_3, x_2 = a_2 \oplus a_3 \Longrightarrow$ thay đổi a_1
    - $x_1 = a_1 \oplus a_3, x_2 \neq a_2 \oplus a_3 \Longrightarrow$ thay đổi a_2
    - $x_1 \neq a_1 \oplus a_3, x_2 \neq a_2 \oplus a_3 \Longrightarrow$ thay đổi a_3
  - Trong 4 TH trên chỉ thay đổi không quá 1 bit

Các kĩ thuật trên ảnh số

- Từ mã a với n bít có thể sửa, k bít thông điệp bí mật x.
- f là hàm băm trích xuất k bít từ một từ mã.
- Ma trận nhúng cho phép tìm được từ mã a' được sửa một cách thích hợp với mọi a và x, sao cho $x = f(a')$ để khoảng cách Hamming:

$$d(a, a') \leq d_{max}$$

- (d_{max}, n, k): là một từ mã với n vị trí được thay đổi trong không quá d_{max} vị trí để nhúng k bit

Các kĩ thuật trên ảnh số

- Thuật toán F5 thực hiện ma trận nhúng chỉ với $d_{max} = 1$.
- Với (1, n, k), các từ mã có độ dài $n = 2^k - 1$. Ta có phân phối thay đổi:

$$D(k) = \frac{1}{n+1} = \frac{1}{2^k}$$

Và tỉ lệ nhúng:

$$R(k) = \frac{k}{n} = \frac{k}{2^k - 1}$$

Các kĩ thuật trên ảnh số

- Sử dụng phân phối thay đổi và tỉ lệ nhúng ta xác định được sự hiệu quả của quá trình nhúng *W(k):*

$$W(k) = \frac{R(k)}{D(k)} = \frac{2^k}{2^k - 1} \cdot k$$

Hiệu quả của quá trình nhúng đối với mã $(1, n, k)$luôn luôn lớn hơn k

Các kĩ thuật trên ảnh số

k	*n*	Mật độ sửa	Tỉ lệ nhúng	Hiệu quả nhúng
1	1	50.00%	100.00%	2
2	3	25.00%	66.67%	2.67
3	7	12.50%	42.86%	3.43
4	15	6.25%	26.67%	4.27
5	31	3.12%	16.13%	5.16
6	63	1.56%	9.52%	6.09
7	127	0.78%	5.51%	7.06
8	255	0.39%	3.14%	8.03
9	511	0.20%	1.76%	9.02

Quan hệ giữa mật độ thay đổi và tỉ lệ nhúng

Các kĩ thuật trên ảnh số

- Hình dưới đây cho thấy sự phụ thuộc giữa các bít thông báo x_i và các vị trí thay đổi bít a_j'.

f(a')	a_1'	a_2'	a_3'
x_1	x		x
x_2		x	x

f(a')	a_1'	a_2'	a_3'	a_4'	a_5'	a_6'	a_7'
x_1	x		x		x		x
x_2		x	x			x	x
x_3				x	x	x	x

Các kĩ thuật trên ảnh số

- Ta xác định hàm băm f:

$$f(a) = \bigoplus_{i=1}^{n} a_i \cdot i$$

- Ta tìm vị trí bit:

$$s = x \oplus f(a)$$

- Kết quả từ mã được thay đổi:

$$a = \begin{cases} a, nếu\ s = 0\ (\leftrightarrow x = f(a)) \\ (a_1, a_2, \dots, a_s, \dots, a_n), ngược\ lại \end{cases}$$

$$a' = \begin{cases} a, nếu\ s = 0\ (\leftrightarrow x = f(a)) \\ (a_1, a_2, \dots, \neg a_s, \dots, a_n), ngược\ lại \end{cases}$$

Các kĩ thuật trên ảnh số

- Mô tả thuật toán F5:
  - Quá trình nhúng:
    - Lấy biểu diễn RGB của ảnh đầu vào
    - Tính bảng lượng tử tương ứng với yếu tố chất lượng của ảnh Q và nén ảnh trong khi lưu các hệ số lượng tử DCT.
    - Tính toán công suất dự kiến khi không có ma trận nhúng:

      $$C = h_{DCT} - \frac{h_{DCT}}{64} - h(0) - h(1) + 0.49h(1)$$

      - h_{DCT} là tất cả các hệ số DCT
      - h(0) là số các hệ số AC DCT bằng 0
      - h(1) là số các hệ số AC DCT có trị tuyệt đối bằng 1
      - $\frac{h_{DCT}}{64}$ là số các hệ số DC
      - $-h(1) + 0.49h(1) = -0.51h(1)$là ước lượng sự hao hụt

Các kĩ thuật trên ảnh số

- Dùng mật khẩu do người dùng xác định trước để sinh ra một mầm cho PRNG nhằm xác định cách nhúng ngẫu nhiên các bít thông điệp. PRNG cũng được sử dụng để sinh một dãy bít giả ngẫu nhiên, dãy bít này sẽ được XOR với thông điệp để tạo nên dãy bít được ngẫu nhiên hóa. Trong suốt quá trình nhúng, bỏ qua các hệ số DC và các hệ số bằng 0.

Các kĩ thuật trên ảnh số

- Chia thông điệp thành các đoạn k bít mà được nhúng thành một nhóm $2^k - 1$ hệ số theo cách ngẫu nhiên. Nếu giá trị băm của nhóm đó không khớp với các bít thông điệp thì giảm giá trị tuyệt đối của một trong các hệ số của nhóm đi 1 để khớp được với dãy bít thông điệp. Nếu hệ số chuyển thành 0 thì gọi là hao hụt và nhúng lại k bít thông điệp giống như vậy vào nhóm hệ số DCT tiếp theo (chú ý là $LSB(d) = d \bmod 2$, với $d > 0$ và $LSB(d) = 1 - d \bmod 2$, với $d < 0$).

Các kĩ thuật trên ảnh số

- Nếu kích cỡ của thông điệp khớp với dung lượng đã ước lượng thì tiến hành nhúng, ngược lại hiển thị thông điệp báo lỗi chỉ rõ độ dài tối đa có thể. Có một số trường hợp ít xảy ra khi dự đoán công suất sai vì sự hao hụt đã dự tính lớn hơn. Trong những trường hợp này, chương trình cần nhúng càng nhiều càng tốt và đưa ra cảnh báo.

Chương 2. Ẩn mã

Các kĩ thuật trên ảnh số

- Ẩn mã trong tệp âm thanh:
  - Ẩn mã trong âm thanh mang những đặc điểm riêng khác với ẩn mã trong các đối tượng đa phương tiện khác. Để đảm bảo yêu cầu cơ bản của ẩn mã thì giấu tin trong tệp âm thanh thuộc vào hệ thống thính giác của con người. Hệ thống thính giác của con người nghe được các tín hiệu ở các dải tần rộng và công suất lớn, đặc điểm này gây khó khăn trong phương pháp giấu tin trong âm thanh
  - Giấu thông tin trong tệp âm thanh đòi hỏi yêu cầu rất cao về tính đồng bộ và tính an toàn của thông tin, các phương pháp giấu thông tin trong âm thanh đều lợi dụng điểm yếu trong hệ thống thính giác của con người

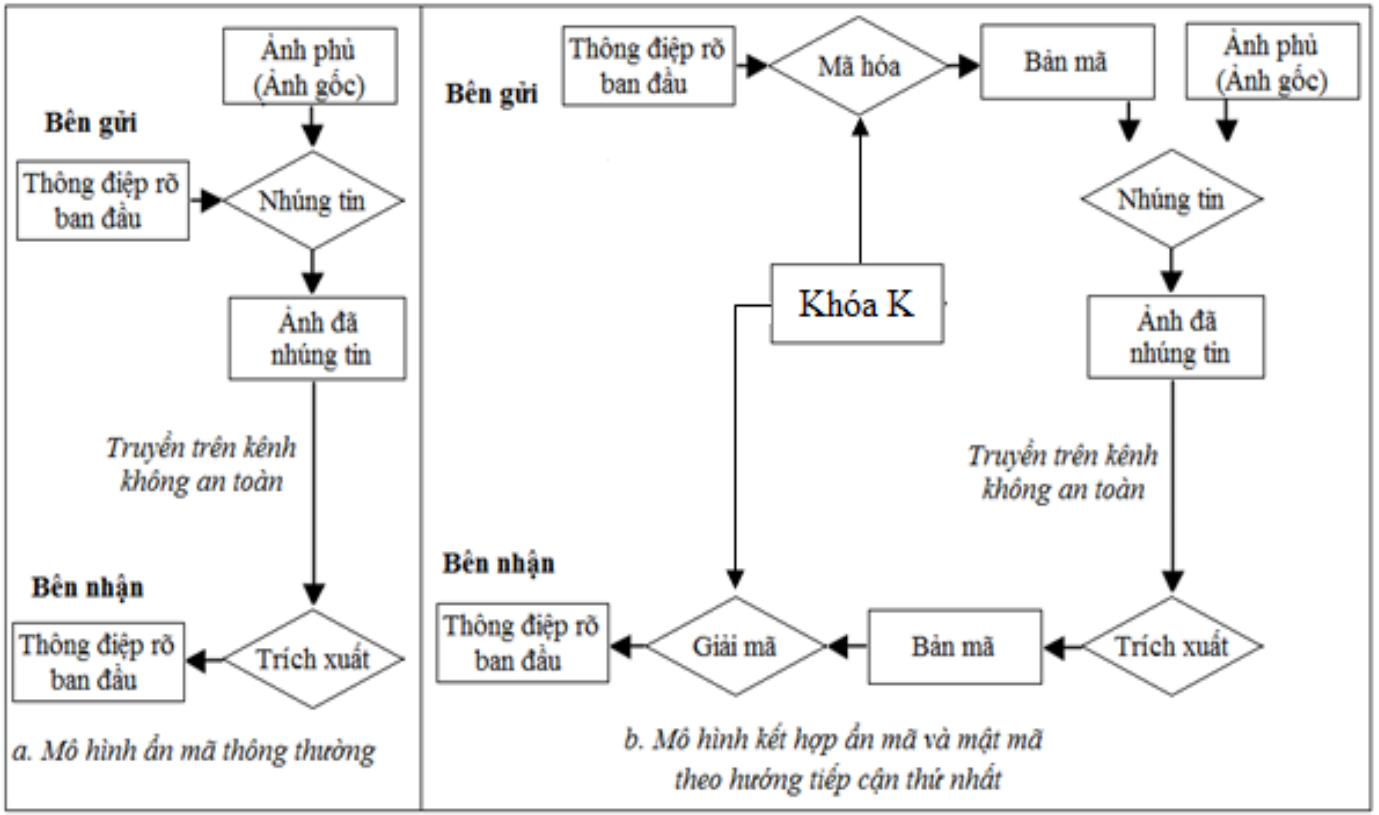
Các kĩ thuật trên ảnh số

- Ẩn mã trong tệp văn bản
  - *Được phân thành 2 hướng:*
    - *Văn bản chứa là văn bản được chụp lại và lưu trên máy như 1 ảnh nhị phân => Kĩ thuật này thực hiện như giấu tin trong ảnh nhị phân*
    - *Phương tiện chứa sử dụng để giấu tin được lưu dưới dạng văn bản*
      - *Ẩn dữ liệu bằng cách dịch chuyển dòng (line shift)*
      - *Ẩn dữ liệu bằng cách dịch chuyển từ (word shift)*
      - *Phương pháp khoảng trắng mở*
      - *Phương pháp cú pháp*
      - *Phương pháp ngữ nghĩa (Semantic methods)*

Chương 2. Ẩn mã

Các kĩ thuật trên ảnh số

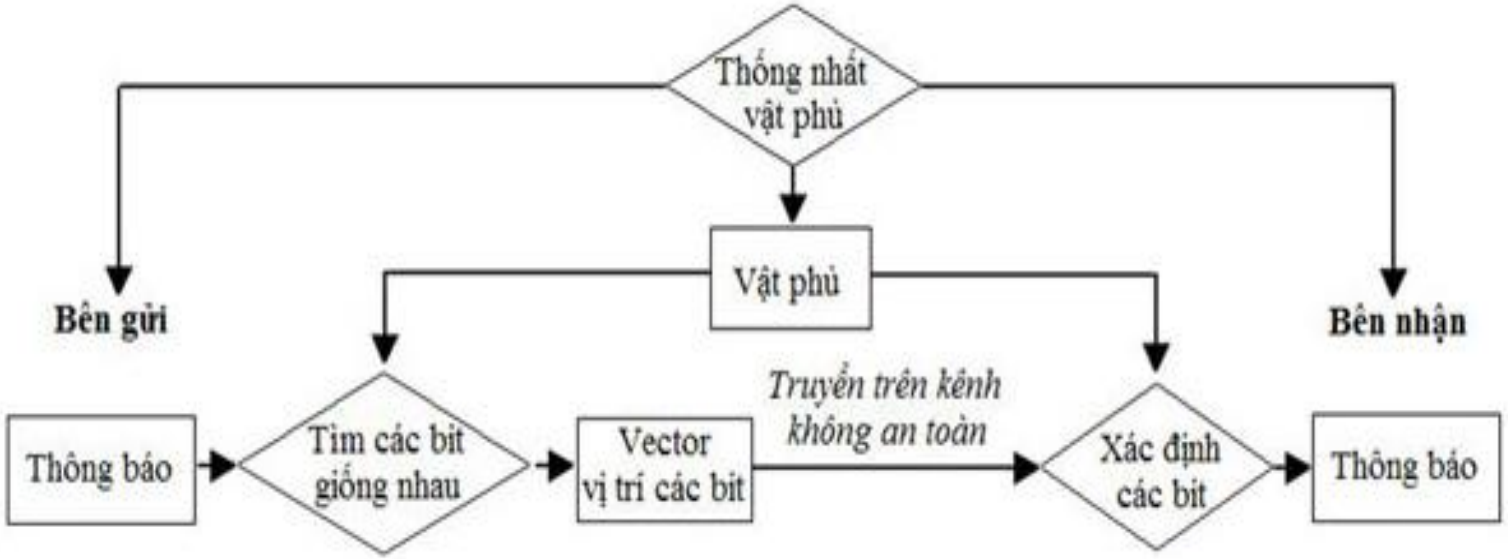
- Kết hợp ẩn mã và mật mã có sửa vật phủ:



Mô hình ẩn mã thông thường và kết hợp với mật mã

Các kĩ thuật trên ảnh số

- Kết hợp ẩn mã và mật mã không sửa vật phủ



Mô hình kết hợp ẩn mã và mật mã không sửa vật phủ

Bài tập lớn

- Lập trình xây dựng chương trình giấu tin mật trong ảnh RGB sử dụng kĩ thuật LSB và trích xuất được tin mật từ ảnh đã được giấu tin
- Lập trình xây dựng chương trình giấu tin mật dùng thuật toán Jsteg