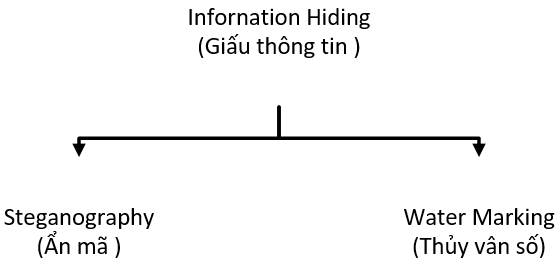
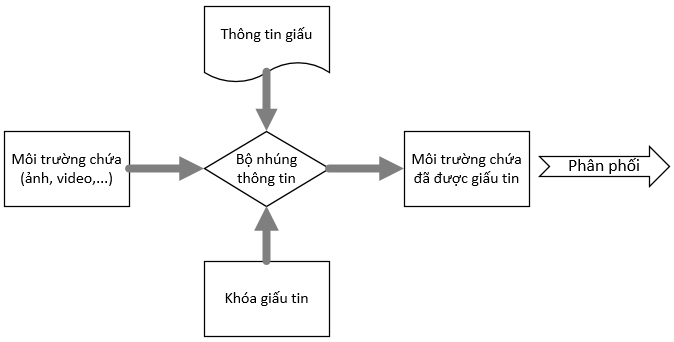
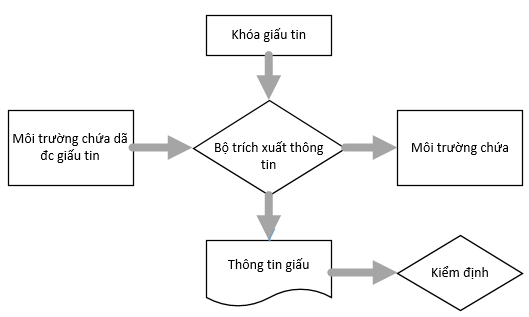
**Câu 1: Nêu khái niệm giấu tin số, trình bày tóm tắt mô hình phân loại giấu tin theo khuynh hướng(thủy vân số và giấu dữ liệu).**

* **K/n:** Giấu tin số (hay còn gọi là giấu) 1 lương thông tin số nào đó vào trong 1 đối tượng dữ liệu số khác.
* **Mô hình phân loại theo khuynh hướng:**
* Ẩn mã là kỹ thuật nhúng tin mật vào môi trường giấu tin
* Thủy vân số là kỹ thuật nhúng dấu ẩn số vào 1 dữ liệu hoặc sản phẩm nhằm chứng thực nguồn gốc hay chủ sở hữu.
* **Mô hình giấu tin cơ bản:**
* ***Quá trình giấu:***

****

* Giau thông tin vào phương tiện chứa
* Thông tin cần giấu tùy theo mục đích của người sử dụng, nó có thể là thông điệp ( với các tin bí mật ) hay logo, hình ảnh bản quyền
* Phương tiện chứa: Các tệp ảnh, text, audio,..là môi trường để nhúng tin
* Bộ nhúng thông tin: Là những chương trình thực hiện việc giấu tin
* Đầu ra: Là phương tiện đã có giấu tin trong đó
* ***Quá trình trích xuất:***



* Diễn ra theo quy trình ngược lại với đầu ra là các thông tin đã được giấu vào phương tiện chứa.
* Sau khi nhận được đối tượng phương tiện chứa có giấu tin, quá trình trích xuất diễn ra thông qua bộ tríc xuất thông tin tương ứng với bộ nhúng thông tin cùng với khóa của quá trình nhúng.
* Kết quả thu được là thông tin đã giấu. Thông tin này được kiểm định và do sánh với thông tin ban đầu

**Câu 2: Các ứng dụng của giấu tin trong thực tế**

* Giấu những thông ti bí mật
* Bảo vệ bản quyền tác giả
* Nhận thức thông tin hay phát hiện xuyên tạc thông tin
* Dấu vân tay hay dán nhãn
* Điều khiển truy cập
* Kiểm soát sao chép
* Điều khiển thiết bị
* Theo dõi quá trình sử dụng
* Theo dõi truyền thông

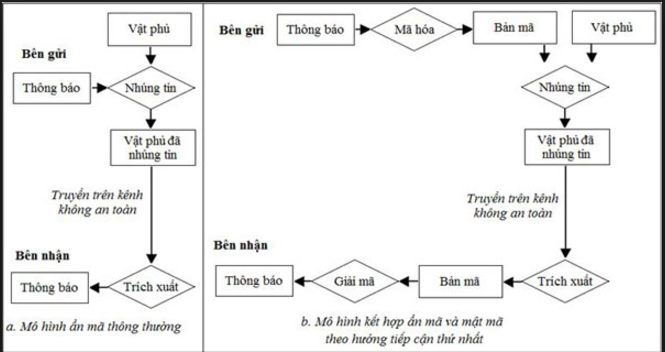
**Câu 3: Trình bày mô hình và tóm tắt nguyên lý ẩn mã**

* **Khái niệm:** Ẩn mã học là một nghệ thuật và khoa học của việc chuyển thông tin bí mật theo cách mà chính sự tồn tại của thông tin mật cần chuyển là không bị phát hiện ra (còn gọi là giấu tin).

**Mô hình:**

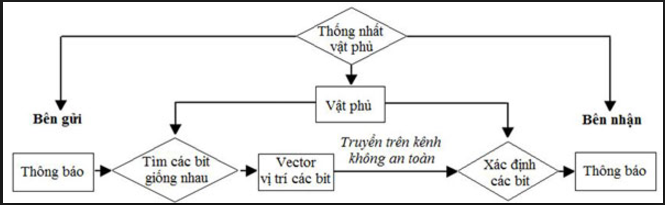
Có hai cách để thực hiện kết hợp ẩn mã và mật mã: thứ nhất là mã hóa thông báo rồi ẩn bản mã này trong vật phủ; thứ hai là xác định những bit giống nhau giữa thông báo và vật phủ sau đó lưu vào các vị trí khác nhau dưới dạng một vector.

- Cách kết hợp thứ nhất đã được sử dụng rất phổ biến. Trước tiên, người gửi mã hóa thông báo bí mật bằng một phương pháp mật mã nào đó để biến thành một bản mã khó hiểu. Sau đó, người gửi tiếp tục sử dụng kĩ thuật ẩn mã để che giấu sự tồn tại của nó trong một vật phủ. Hình dưới đây mô tả quá trình thực hiện của cách thức này so với phương pháp ẩn mã thông thường (không dùng mật mã).



Theo mô tả trong hình, ở cách kết hợp với mật mã thì mô hình có thể tạo nên sự bảo vệ hai lớp, ngoài việc giấu đi nội dung thực của thông báo, thì do có ẩn mã nên kẻ tấn công khó có thể biết được sự có mặt của bản mã đó trong vật phủ.

- Cách kết hợp thứ hai sử dụng lược đồ hoàn toàn khác, có phần mới lạ và đặc biệt hơn rất nhiều. Sau khi bên gửi và bên nhận thống nhất một vật phủ thì người gửi sẽ xác định các bit của thông báo bí mật mà trùng khớp với các bit trong vật phủ rồi lưu vào thành một vector chứa các vị trí khác nhau của vật phủ. Thông tin truyền đi chỉ đơn giản là vector này chứ không phải là thông báo ban đầu hay vật phủ. Phương pháp này chính là sự kết hợp ẩn mã và mật mã không sửa vật phủ.



Đầu tiên, bên gửi và bên nhận đồng ý sử dụng một vật phủ. Người gửi không phải chỉnh sửa vật phủ, mà chỉ xác định những bit của thông báo bí mật nào giống với các bit trong vật phủ, thì lưu vào các vị trí khác nhau (chẳng hạn trong vật phủ) dưới dạng một vector. Vector này sau đó được gửi (thậm chí có thể tăng cường sự an toàn bằng cách mã hóa vector) cho người nhận. Khi ấy, kẻ tấn công có thể chặn được vector đã gửi (có thể đã được mã hoá) nhưng không thể biết được vật phủ tương ứng. Vì vậy, để phá được lược đồ ẩn mã này, kẻ tấn công không những phải chặn được thông tin bí mật đã gửi mà còn phải biết được vật phủ.

* **Các nguyên lý ẩn mã:**
* Ẩn mã thuần túy: Bộ 4 δ = (C,M,D,E)

Trong đó: C là tập các vaath phủ có thế

M là tập các thông điệp mật với |C| ≥ |M|

E: C x M -> C là hàm nhúng tin

D: C-> M là hàm trích xuất tin với D(E(c,m)) = m với (với mọi m € M và c € C ddc gọi là hệ ẩn mã thuần túy.

* Ẩn mã bí mật: Bộ 5 δ =(C,M,K, Dk,Ek)

Trong đó: C: Tập các vật phủ có thể

M: Tập các thông điệp mật

K: Tập các khóa bí mật.

Ek: C x M x K -> C và Dk : C x K -> M với Dk (Ek(c,m,k),k))=m

Với mọi m € M, c € , k € K đc gọi là 1 hệ ẩn mã khóa bí mật

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

**Câu 4: Tóm tắt Quá trình xử lý ảnh nén jpeg(7 bước)**

**Bước 1:** Chuyển đổi ảnh sang YcbCr

* Chuyển đổi các lớp mẫu RGB của hình ảnh vào 3 thành phần khác nhau (Y,Cb,Cr)
* Y liên quan tới độ sáng và 2 thành phần màu U,V
* Các công thức có thể dùng để tính toán y,U và V từ R,G,B

Y = 0,299R + 0,587G + 114B

U = 0,492(B-Y) = -0,147R – 0,289G + 0,436B

V = 0.877(R-Y) = 0,615R – 0,515G – 0,100B

**Bước 2:** Giả giá trị thành phần màu: mục đích để giảm kích cỡ ảnh

* Mắt ng thường nhạy cảm với những thay đổi về độ sáng là những thay đổi về màu sắc -> giảm kích cỡ tổng thể của tệp thường sử dụng cách giảm chất lượng màu

**Bước 3:** Chuyển các giá trị điểm ảnh sang tần số.

* Phép biến đổi Fourier(DFT), Cosin rời rạc(DCT) đc sử dụng để ánh xạ 1 tín hiệu vào miền tần số
* DFT thường đc sử dụng trong xử lý âm thanh
* DCT thường đc sử dụng cho việc xử lý hình ảnh để biến đổi chúng thành tần số
* DCT biến đổi dữ liệu dưới dạng biên độ thành dữ liệu dưới dạng tần số
* Mục đích dữ liệu của ảnh còn tập trung vào 1 phần nhỏ các hệ số hàm truyền

|  |  |
| --- | --- |
| DCT 1 chiều | DCT 2 chiều |
| +) Quá trình biến đổi DCT thuận  X(R) = C(k)  +) Hàm biến đổi DCT ngược  x(m) = C(k)  Trong đó: X(k) : chuỗi kết quả  x(m): Gtri của mẫu m  k : Chỉ số của hệ số triển khai  N : Só mẫu có trong tín hiệu  C(k)= nếu k = 0 và = 1 nếu k#0 | +) Quá trình biế đổi DCT thuận  F(u,v)=.f(j,k)cos  Trong đó: f(j,k): MẪu gốc trong khối điểm ảnh cỡ 8x8  F(u,v): Các hệ số của khối DCT 8x8  C(u),C(v)= nếu u,v=0 và =1 neeud u,v #0  u,v = 0 -> F(u,v)= f(j,k)  +)Biến đổi nghịch  F(j,k)=cos |

**Bước 4: Lượng tử hóa**

* **Mục đích:** Để lượng tử giá trị biểu thị cho hình ảnh sau giai đoạn chuyển đổi ảnh sang tần số
* Sau quá trình này 1 lượng lướn dữ liệu có thể đc loại bỏ mà không ảnh hưởng đến chất lượng của ảnh

Hệ số ượng tử hóa: Fq (u,v)= []= số nguyên tố gần nhất[]

**Bước 5: Sắp xếp zíc zắc**

* Nhằm biến đổi mảng 2 chiều thành chuỗi số 1 chiều
* Sau khi lượng tử các hệ số DCT chỉ có 1 vài giá trị được giữ lại là # 0, đa số sẽ luôn luôn là số 0
* Sắp xếp zíc zắc lại các hệ số trên để các tần số lượng tử đc nhóm lại với nhau

**Bước 6: Mã hóa độ dài chạy (RLC)**

* Thành phần AC sau khi quét zic zắc thì các giá trị 0 giống nhau đc thay = mã RLC
* Dấu EOB đánh dấu vị trí ban đầu của chuỗi các số liên tiếp
* Nguyên tắc:

B1. Phát hiện loạt (loạt các giá trị giống nhau) cụ thể trong các giá trị 0 trước mỗi giá trị # 0

B2. Kí hiệu mã

**Bước 7: Mã hóa dộ dài thay đổi (VLC)**

* Mã hóa thành phần DC
* Mã hóa thành phần AC

**Câu 9: Trình bày về phân tích ẩn mã dựa trên điều tra số**

* Người phân tích có thể xác định một cách tân công thời điểm 2 bên gửi và nhận các thông điệp bí mật được che giấu
* Đầu tiên người phân tích cố gắng khôi phục lại một số thuộc tính của thông điệp được nhúng và các tính chất của thuật toán ẩn mã
* Các đặc tính của những thay đổi khi thưc hiện nhúng cũng tiết lộ các thông tin về cơ chế nhúng
* Cuối cùng người phân tích có thể đoán được phương pháp ẩn mã được sử dụng và sẽ cố gắng xác định khóa nhúng để trích xuất ra thông điệp

**Câu 10: Nêu ý nghĩa của việc phân tích ẩn mã, so sánh giữa kỹ thuật phân tích mù và kỹ thuật phân tích có chủ đích trong ẩn mã**

* Ý nghĩa của việc phân tích ẩn mã
* So sánh giữa kỹ thuật phân tích mù và kỹ thuật phân tích có chủ đích trong ẩn mã

**Khác:**

|  |  |
| --- | --- |
| Phân tích có chủ đích | Phân tích mù |
| * Biết được thuật toán đang được dùng * Thiết kế các đặc tính cho phân tích ẩn mã có chủ đích hầu như luôn bắt đầu với việc phân tích toán nhúng để định lượng kết quả của các phương pháp nhúng tin | * Không biết được thuật toán ẩn mã đang được sử dụng * Lựa chọn các đặc trưng để phân tích * Huấn luyện bộ phận phân loại phân tích ẩn mã mù |

**Giống:** lựa chọn đại diện đặc trưng và xác định ranh giới quyết định

**Câu 11: Nêu những cải tiến của thuật toán outless so với jstec**

* Phân tán các vị trí trên toàn bộ hình ảnh thông qua một bộ sinh số giả ngẫu nhiên PK trên ảnh c và sử dụng mầm khóa k

**Câu 12: Nêu khái niệm, ý nghĩa của thủy vân số**

1. ***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 đối tượng đó.

- Mục đích của thủy vân số là bảo vệ bản quyền cho phương tiện dữ liệu số mang thông tin thủy vân

***b. Ý nghĩa của thủy vân số***

* Bảo vệ quyền tác giả: Trong thực tế, nhiều tác phẩm đã có tác quyền nhưng vẫn bị sử dụng sai mục đích. Các thông báo tác quyền này thường được đặt ở vị trí nào đó trên tác phẩm được phân phối. Vấn đề bảo vệ bản quyền này không được đảm bảo vì không quá khó để loại bỏ nó ra khỏi một tài liệu khi cần sao chép.

Do các dấu thủy vân có thể vừa không nhìn thấy vừa không thể tách rời sản phẩm chứa nó nên sẽ là giải pháp tốt cho việc bảo vệ quyền tác giả. Dấu thủy vân(có một thông tin nào đó mang ý nghĩa quyền sở hữu tác giả), sẽ được nhúng vào trong các sản phẩm, dấu thủy vân đó chỉ người chủ sở hữu hợp pháp mới có và được dùng làm minh chứng cho bản quyền sản phẩm

* Xác thực thông tin và phát hiện xuyên tạc thông tin

Dấu thủy vân sẽ được nhúng trong 1 tác phẩm sau đó được lấy ra và so sánh với dấu thủy vân ban đầu. Nếu có sự sai lệch chứng tỏ tác phẩm gốc đã bị tấn công và xuyên tạc.

Các thủy vân nên được ẩn để tránh sự tò mò của đối phương

* Dấu vân tay hay dán nhãn: thủy vân còn được sử dụng để nhận diện người gửi hay người nhận một thông tin nào đó. Ví dụ các vân khác nhau sẽ được nhúng vào các bản copy khác nhau của thông tin gốc trước khi chuyển cho nhiều người
* Điều khiển truy nhập : các thiết bị phát hiện thủy vân(ở đây sử dụng phương pháp phát hiện thủy vân đã dấu mà không cần thông tin gốc) được gắn sẵn vào trong các hệ thống đọc ghi, tùy thuộc vào việc có thủy vân hay không để điều khiển truy cập

**Câu 13: So sánh ẩn mã và thủy vân số**

* **Giống**: giấu 1 dữ liệu trong dữ liệu khác
* **Khác**: về mục đich

+ Ẩn mã: che giấu sự tồn tại của dữ liệu đc nhúng

+ Thủy vân số: đảm bảo tính xác thực, an toàn, và bảo vệ bản quyền đối với dữ liệu chứa thông tin được nhúng

|  |  |
| --- | --- |
| Ân mã | Thủy vân số |
| Mục đích là bảo vệ thông tin | Mục đích là bảo vệ môi trường giấu tin |
| Giau được càng nhiều thông tin càng tốt, ứng dụng trong truyền dữ liệu thông tin mật | Chỉ cần thông tin đủ để đặc trưng cho bản quyền của chủ sở hữu |
| Thông tin được giấu phải ẩn, không cho người khác thấy được bằng mắt thường | Thông tin giấu có thể ẩn( thủy vân ẩn ) hoặc hiện ( thủy vân hiện) |
| Chỉ tiêu quan trọng nhất là dung lượng được giấu | Chỉ tiêu quan trọng nhất là tính bền vững của tin được giấu |

**Câu 14: Sự phân loại thủy vân và sự tóm tắt từng loại**

• Dựa theo miền thực hiện, chia thành 2 loại:

- Thủy vân trên miền không gian: là thủy vân thực hiện nhúng trực tiếp vào các giá trị của vật phủ

- Thủy vân dực trên miền tần số: là thủy vân thực hiện nhúng vào hệ tần số tương ứng của các giá trị vật phủ, tức là trước khi nhúng cần biến đổi các giá trị của vật phủ sang miền tần số thông qua các biến đổi, chẳng như: DCT, DWT,…

• Dựa theo môi trường chứa:

- Thủy vân trong ảnh

- Thủy vân trong âm thanh

- Thủy vân trong video

- Thủy vân trong vân bản

• Dựa theo sự cảm nhận của con người:

- Thủy vân ẩn: là thủy vân sau khi được nhúng vào vật phủ chúng ta không thể nhìn thấy cũng như không có cảm nhận được sự thay đổi của vật chứa thủy vân so với vật phủ ban đầu

- Thủy vân hiện: là thủy vân sau khi nhúng vào vật phủ chúng ta hoàn toàn có thể nhìn thấy hoặc cảm nhận được

- Trong thủy vân ẩn: gồm 3 loại:

+ Thủy vân bền vững: là thủy vân được nhúng theo cách dù thay đổi trên vật phủ nhưng giác quan của con người không cảm nhận được và nó có thể chịu được mọi loại tấn công, đồng thời chỉ có thuật toán phù hợp mới có thể khôi phục được thủy vân này

+ Thủy vân dễ vỡ: là thủy vân mà bất kì thao tác thay đổi hay sửa chữa nào cũng sẽ làm hỏng hoặc làm biến đổi thủy vân, tức là nó không chịu được bất kì tác động hay tấn công nào

+ Thủy vân bán dễ vỡ: là thủy vân có thể chịu được 1 số phép biến đổi hợp pháp hoặc 1 số loại tấn công nào đó chứ không phải tất cả các biến đổi hay mọi loại tấn công

**Câu 15: Trình bày cấu trúc của hệ thống thủy vân nói chung, có nhận xét gì về quá trình thực hiện trong hệ thống đó**

Mỗi hệ thống thủy vân luôn bao gồm ít nhất 2 quá trình tách biệt nhúng thủy vân và phát hiện/trích xuất thủy vân:

**Câu 16: Trình bày lược đồ nhúng và trích xuất thủy vân, ghi rõ công thực nhúng, trích xuất và giải thích các tham số**

• Lược đồ nhúng

I: vật phủ dùng để nhúng thủy vân vào

Ir: vật có nhúng thủy vân nhưng bị tấn công trên đường truyền

Emb: hàm nhúng thủy vân

W: thủy vân ban đầu cần nhúng

In: vật phủ sau khi được nhúng thủy vân

K: khóa sử dụng trong quá trình nhúng và trích xuất thủy vân

• Lược đồ trích xuất

I: vật phủ dùng để nhúng thủy vân vào

Ir: vật có nhúng thủy vân nhưng đã bị tấn công trên đường truyền

Dtc: hàm trích xuất thủy vân

K: khóa sử dụng trong quá trình trích xuất thủy vân

Wc: thủy vân trích xuất được

W: thủy vân ban đầu cần nhúng

**Câu 17: Trình bày các tính chất cơ bản của thủy vân số, vì sao cần phải có sự cân bằng giữa các tích chất này trong 1 hệ thống thủy vân số**

**• Tính chất:**

- ***Bền vững:***

+ Không bị thay đổi trước các tác động xử lí cũng như các tấn công đồng thời 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

***- Dung lượng nhúng:***

+ Là số lượng thông tin có thể được giấu trong vật phủ

+ Luôn luôn phải xem xét tới 2 yêu cầu quan trọng khác đó là tính trong suốt và tính bền vững

=> Để có được dung lượng nhúng thường phải mất đi tính bền vững hoặc tính trong suốt hoặc cả hai

- ***Trong suốt:*** Không thể cảm nhận được bằng các giác quan thông thường của con người với các thông tin đã được nhúng

- ***An toàn:*** Chỉ những người dùng có thẩm quyền mới có thể phát hiện, trích xuất và thậm chỉ sửa đổi

- ***Chi phí cao:***

+ Độ phức tạp của thuật toán sử dụng trong mô hình thủy vân

+ Vấn đề rất quan trọng đặc biệt trong các ứng dụng giám sát truyền thông vì khi đó việc sản xuất đa phương tiện không được phép chậm và quá trình phát hiện thủy vân phải thực hiện với thời gian thực.

• ***Cần phải có sự cân bằng giữa các tích chất này trong 1 hệ thống thủy vân số vì:*** Một tính chất nào đó có thể lại đổi ngược với tính chất khác, chẳng hạn khi tăng dung lượng nhúng thì ảnh hưởng tới tính trong suốt của thủy vân

**18- So sánh thủy vân trên miền không gian, miền tần số**

* **Thủy vân trên miền không gian**:
* Sửa đổi trực tiếp các giá trị điểm ảnh trên miền không gian của ảnh.
* Đơn giản và không cần ảnh phủ để trích xuất thủy vân
* Không bền vững để chống lại các phép xử lý ảnh bởi vì thủy vân không được phân phối trên toàn bộ ảnh và do đó các phép xử lý ảnh có thể dễ dàng phá hủy thủy vân
* **Thủy vân trên miền tần số**:
* Chèn 1 thủy vân vào các hệ số tần số của các ảnh được biến đổi thông qua các phép biến đổi Fourier rời rạc, Cosine rời rạc hay sóng rời rạc.
* Thường bền vững hơn trước các phép biến đổi ảnh. Vì phần lớn năng lượng tập trung vào các thành phần có tần số thấp
* Ít bị tác động khi thực hiện các thao tác xử lý, xử lý ảnh trên ảnh có chứ thủy vân
* Tương đối bền vững
* 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

**19- Trình bày thuật toán thủy vân dựa trên phương pháp thay thế LSB trên miền không gian.**

H: ảnh phủ mức xám có kích thước N x M

W: ảnh thủy vân nhị phân kích thước N x M

L: số bit được sử dụng trong mức xám của các điểm ảnh

(+): phép toán thay thế các bit của thủy vân vào các LSB của ảnh phủ

*Thuật toán*:

1. Lấy các điểm ảnh từ ảnh phủ:

H = {h(i,j); 0≤ i,j < N} , h(i,j) {0,1,2,…, }

1. Lấy các điểm ảnh từ thủy vân

W = {w(i,j) , 0≤ i,j < M}

1. Thay thế LSB của các điểm ảnh trong ảnh phủ bởi các bit của thủy vân

= {} , (i,j) {0,1,2,…, }

**20- Trình bày phương pháp thủy vân dựa trên phép cộng trên miền không gian**

* Không xét những bit cụ thể của 1 điểm ảnh
* Cộng 1 lượng giá trị thủy vân vào 1 điểm ảnh trong quá trình nhúng
* (i,j) = h(i,j) + a(i,j) \* w(i,j) trong đó {a(i,j)} là hệ số tỷ lệ
* Nếu a( i,j) lớn thì ảnh có chứa thủy vân sẽ bị méo

+ Không nhúng 1 giá trị lớn vào 1 điểm ảnh đơn mà phải nhúng vào 1 khối điểm ảnh

+ Trước khi được nhúng sẽ chia cho kích cỡ khối ảnh đề giảm giá trị

* Sử dụng ảnh tham chiếu khi trích xuất

+ Vì họ không biết được vị trí đã nhúng nên rất khó có thể xác định được thủy vân

**21- So sánh phương pháp thủy vân thay thế LSB và phương pháp cộng trong miền không gian. Tại sao khi sử dụng phương pháp cộng trong miền không gian để nhúng 1 thủy vân có giá trị lớn thì lại thường lựa chọn nhứng vào 1 khối ảnh thay vì 1 điểm ảnh đơn**

|  |  |
| --- | --- |
| **PP thay thế LSB** | **PP cộng** |
| * Vị trí các bit được xác định trước * Sử dụng ảnh gốc * Không với qua được các tấn công thêm nhiễu hoặc nén dữ liệu | * Không xét những bit cụ thể * Sử dụng ảnh tham chiếu * Ảnh chứa thủy vân sẽ bị méo |

*Khi sử dụng phương pháp cộng trong miền không gian để nhúng 1 thủy vân có giá trị lớn thì lại thường lựa chọn nhứng vào 1 khối ảnh thay vì 1 điểm ảnh đơn VÌ:*

Nếu a(i,j) lớn thì ảnh có chứa thủy vân sẽ bị méo và như vậy rất khó để có thể đạt được độ trong suốt cao.

**Câu 22: Trình bày thuật toán thủy vân dựa trên phương pháp thay thế trên miền tần số, có nhận xét gì về khối ảnh và số khối thủy vân sau khi được chia nhỏ.**

* Thủy vân có thể được áp dụng trong miền tần số bằng cách trước tiên sử dụng một phép biến đổi, các giá trị tần số đặc biệt của ảnh phủ sẽ được sửa đổi để chèn thủy vân vào đó.
* Vì các thánh phần tần số cao thường bị mất khi nén hoặc thay đổi kích thước ảnh nên thủy vân được nhúng vào các thanh phần có tần số thấp hơn hoặc vào các thành phần có tần số chứa thông tin quan trọng của ảnh.
* Thuật toán :

Cho Hmvà Wn  tương ứng là các ảnh chia nhỏ ra từ ảnh phủ H cỡ N x M và thủy vân W cỡ MxM.Hm\_DCT là ảnh sau khi biến đổi Hm bởi phép DCT và Hm\_F là ảnh sau khi nhúng Wn vào Hm\_DCT. Phương pháp thay thế trong miền tần số thực hiện như sau:

1. Chia ảnh phủ thành các khối ảnh có kích thước 8x8

H = { h(i,j), 0 ≤ i, j < N}

Hm = {hm ( i, j), 0 ≤ i,j <8} trong đó hm (i, j)

€ { 0,1,2,…, 2L – 1 } và m là tổng số các khối 8x8

1. Cách chia thủy vân thành các khối ảnh có kích thước 2 x 2

W = { w (i,j), 0 ≤ i, j<M }

Wn = { wn( i,j), 0 <i, j<2 }, trong đó wn (i, j) € { 0,1} và n là tổng khối 2x2

1. Sử dụng công thức DCT để chuyên Hm thành Hm\_DCT
2. Chèn Wm vào các hệ số của Hm\_DCT

Hm\_F = { hm\_F (i,j) = hm\_DCT (i, j) ( kí hiệu OR) wm (i,j) , 0 ≤ i, j<8}

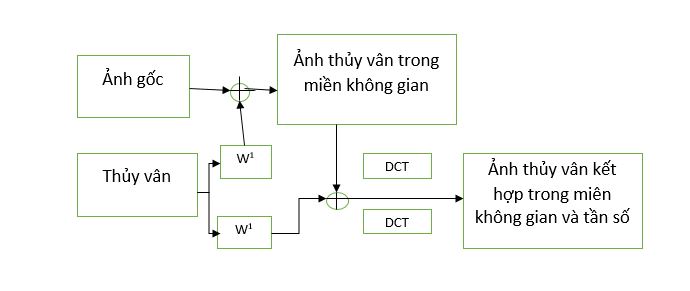
1. Ap dụng phép biến đổi DCT ngược để chuyển ảnh có chứa thủy vân Hm\_F  về dạng ảnh thông thường

Nhận xét : ???

**Câu 23: Ý tưởng kết hợp thủy vân trong miền không gian và tần số có sự cải tiến như thế nào so với việc sử dụng từng phương pháp riêng biệt?**

* Thủy vân trong miền không gian chỉ đơn giản là chèn thủy vân nằng cách thay đổi các mức xám của một số điểm ảnh trong ảnh phủ, tuy nhiên phương pháp này không bền vững đối với các cuộc tấn công.
* Đối với thủy vân trong miền tần số thì chúng ta lại chèn thủy vân vào các hệ số của ảnh đã biến đối thông qua các phép biến đổi DCT, DFT, và DWT. Nhìn chung, phương pháp thủy vân trong miền tần số bền vững đối với các cuộc tấn công nhưng lại không nhúng được nhiều thông tin bởi chất lượng ảnh sẽ bị giảm đáng kể sau khi thực hiện chèn thủy vân
* Để giải quyết được nhược điểm của hai phương pháp trên, người ta đã thực hiện kết hợp thủy vân trong cả miền với nhau. Y tưởng là tách ảnh thủy vân ra thành hai phần tương ứng với việc chèn trong miền không gian và tần số dựa trên sự ưu tiên của người dùng và mức độ quan trọng của dữ liệu .

Sơ đồ luồng của phương pháp kết hợp thủy vân trong miền không gian và tần số ( Tr.136\_H.4.16)



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

**Câu 24: Trình bày thuật toán kết hợp thủy vân trong miền không gian ,tần số.**

Gỉa sử H là ảnh phủ mức xám có kích thươc NxN và W là ảnh thủy vân ở dạng nhị phân có kích thước MxM . Chúng ta sử dụng một số kí hiệu sau:

* W1 và W2 là hai thủy vaab được tách ra từ W
* Hs  là ảnh kết hợp từ H và W1 trong miền không gian
* HDCT là ảnh trong đó HS được biến đổi snag miền tần số theo phép biến đổi DCT
* HF là ảnh nhận được khi kết hợp HDCT và W2 trong miền tần số
* OR : Là phép toán thay thế các bit của thủy vân số vào các LSB của ảnh phủ

Thuật toán thủy vân kết hợp hai miền không gian và tần số như sau :

1. Tách thủy vân thành hai phần:

W = {w(i,j), 0 ≤ i, j <M}, trong đó w(i, j) € {0, 1}

W1 = {w1(i,j), 0 ≤ i,j < M1} trong đó w1 (i, j) € {0,1}

W2 = { w2(i,j, 0≤ i,j < M2)} trong đó w2 (i, j) € {0,1}

M = M1 + M2

1. Chèn W1 vào miền không gian của H để thu được HS

HS = { hS (i,j) = h(i,j) OR w1 (i, j), 0 ≤ i, j < N}, trong đó h(i,j) và hS (i,j) € {0, 1, 2,…, 2L - 1 }, và L là số bit đã dùng trong mức xám của các điểm ảnh.

1. Biến đổi HS thành HDCT theo phép biến đổi DCT
2. Chèn W2 vào các hệ số của HDCT thành HF

HF = { hF (i,j) = hDCT OR w2 (i, j), 0 ≤ i, j < N}, trong đó hF (i,j) € {0, 1, 2,…, 2L - 1 }

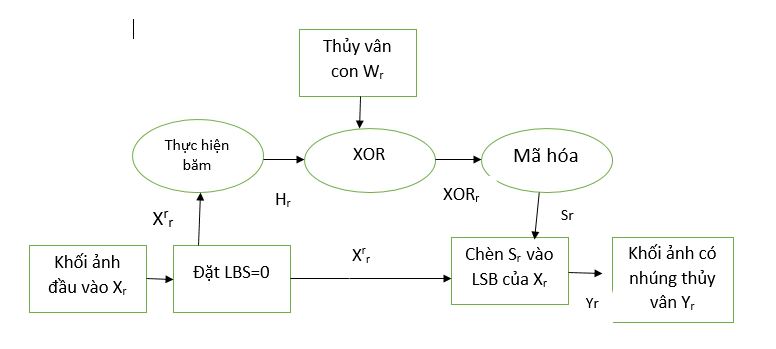
1. Biến đổi ảnh có nhúng thủy vân số ở dạng DCT về dạng bình thường bằng phép biển đổi DCT ngược.

**Câu 25: Trình bày thuật toán và vẽ sơ đồ mô tả thuật toán nhúng/trích xuất thủy vân dễ vỡ dựa trên khối của con**

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. Thuật toán của Wrong có sử dụng thuật toán mã hóa công khai RSA và MD5 đối với hàm băm

* ***Thuật toán nhúng thủy vân dễ vỡ dựa trên khối***

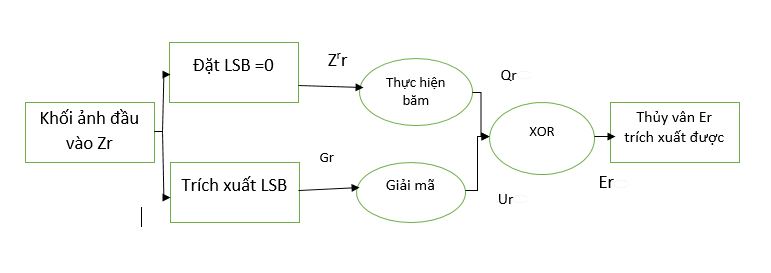
Sơ đồ thực hiện nhúng thủy vân( H.4.17/tr.137)



1. Chia ảnh gốc X thành các ảnh con Xr
2. Chia thủy vân W thành các thủy vân con Wr
3. Với mỗi ảnh con Xr , đặt LSB thành bít 0 để nhận được X’r
4. Với mỗi X’r, dùng hàm băm ( MD5 or SHA ) để nhận được mã băm Hr
5. XORr là kết quả nhận được khi thực hiện XOR Hr với Wr
6. Mã hóa XORR là kết quả nhận được khi thực hiện XOR HR với Wr
7. Nhúng Sr vào LSB của X’r  để thu được ảnh con có thủy vân Yr

* ***Thuật toán trích xuất thủy vân***

Sơ đồ thực hiện nhúng thủy vân( H.4.18/tr.138)



* ***Thuật toán trích xuất :***

1. Chia ảnh Z nhận được thành các ảnh con Zr
2. Đặt LSB của Zr thành bít 0 kết quả thu được là Zr’
3. Trích xuất LSB của Zr  nhận được Gr
4. Giai mã Gr bằng cách dùng RSA với khóa công khai K để thu được Ur
5. Với mỗi Zr’ sử dụng hàm băm để nhận được mã băm tương ứng Qr
6. XOR Qr với Gr để trích xuất thủy vân Er

* Thuật toán thủy vân dễ vỡ dựa trên khối của Wong có điểm yếu đó là các khối ảnh độc lập với nhau. Do đó kẻ tấn công có thể lợi dụng nhược điểm này để thực hiện tấn công giả mạo ra một ảnh mới nhưng vãn không hè tác động tới thủy vân dễ vỡ đã được nhúng. Vì vậy , bằng cách này thủy vân đã nhúng trong ảnh không thay đổi