Lý thuyết

**Câu 1: Định nghĩa ẩn mã thuần túy. Tại sao lực lượng vật phủ ít nhất phải bằng lực lượng của thông điệp?**

-Ẩn mã thuần túy

Bộ bốn , trong đó C là tập các vật phủ có thể, M là tập các thông điệp mật với

là hàm nhúng tin và là hàm trích xuất tin với tính chất:

với và được gọi là hệ mã thuần túy

-Lực lượng vật phủ ít nhất phải bằng lực lượng của thông điệp vì nếu như lực lượng vật phủ nhỏ hơn lực lượng của thông điệp thì nghĩa là vật phủ sẽ được sử dụng để nhúng nhiều lần các thông điệp đó là điều tối kị. Nên người ta thường chỉ nhúng 1 thông điệp trong một ảnh chứ không sử dụng lặp lại để nhúng các thông điệp khác rồi truyền đi, và thường không sử dụng những bức ảnh public trên mạng mà hay sử dụng những bức ảnh của mình để tăng độ an toàn hơn.

**Câu 2: Trình bày định nghĩa ẩn mã khóa bí mật. Tại sao lực lượng của tập vật phủ lại không nên nhỏ hơn lực lượng của tập thông điệp?**

-Ẩn mã khóa bí mật

Bộ bốn , trong đó C là tập các vật phủ có thể, M là tập các thông điệp mật với , K là tập các khóa bí mật.

Hàm nhúng tin và hàm trích xuất tin với tính chất:

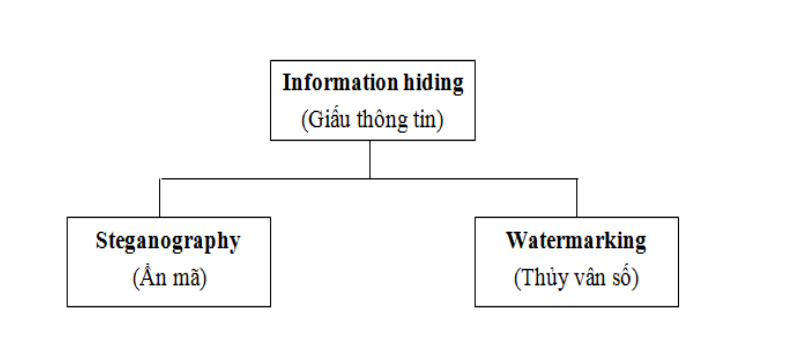
với và và được gọi là hệ ẩn mã khóa bí mật

-Lực lượng vật phủ không nên nhỏ hơn lực lượng của thông điệp vì nếu như lực lượng vật phủ nhỏ hơn lực lượng của thông điệp thì nghĩa là vật phủ sẽ được sử dụng để nhúng nhiều lần các thông điệp đó là điều tối kị. Nên người ta thường chỉ nhúng 1 thông điệp trong một ảnh chứ không sử dụng lặp lại để nhúng các thông điệp khác rồi truyền đi, và thường không sử dụng những bức ảnh public trên mạng mà hay sử dụng những bức ảnh của mình để tăng độ an toàn hơn.

**Câu 3: Trình bày khái niệm về giấu tin số, vẽ và trình bày tóm tắt mô hình phân loại giấu tin theo khuynh hướng.**

-Giấu tin số là kĩ thuật nhúng một lượng thông tin số vào trong một đối tượng dữ liệu số khác.

-Mô hình phân loại giấu tin theo khuynh hướng



Phân loại

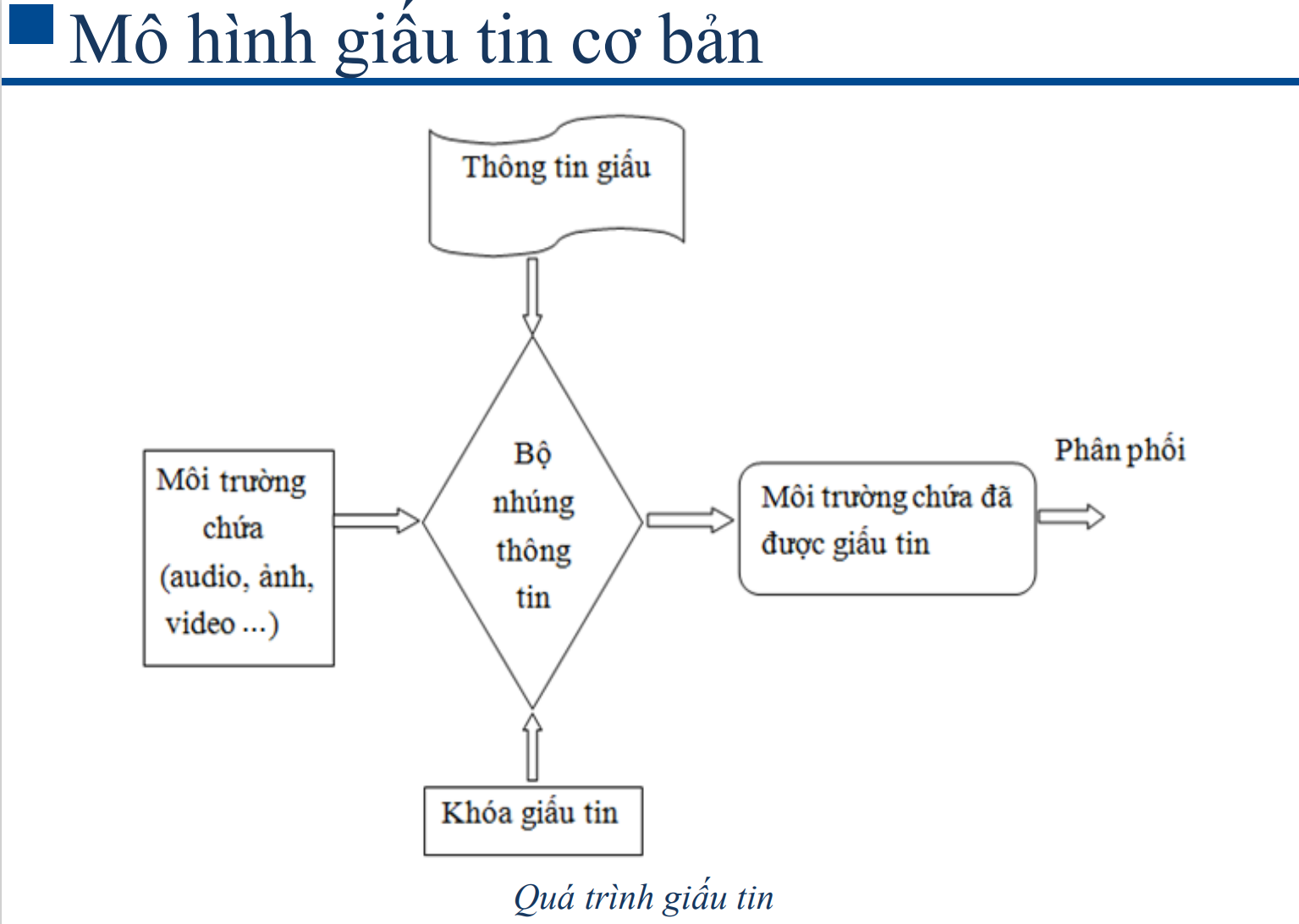
-Ẩn mã để bảo mật cho dữ liệu được đem giấu

-Thủy vân số bảo vệ cho chính đối tượng mang tin giấu, để bảo vệ bản quyền cho đối tượng mang tin

**Câu 4: Trình bày tóm tắt quá trình giấu và trích xuất thông tin của mô hình giấu tin cơ bản.**

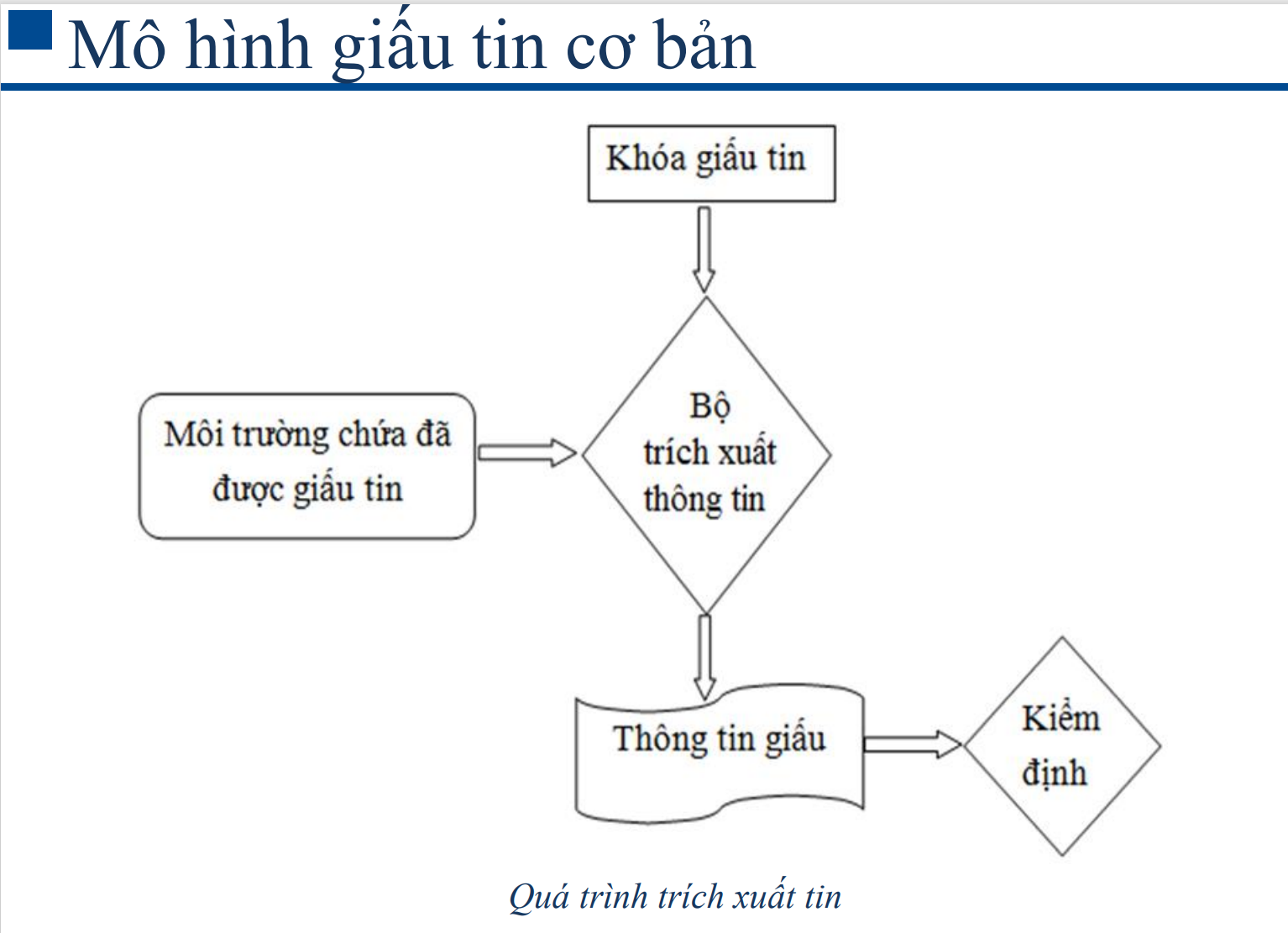
-Mô hình giấu tin cơ bản

+Quá trình giấu tin



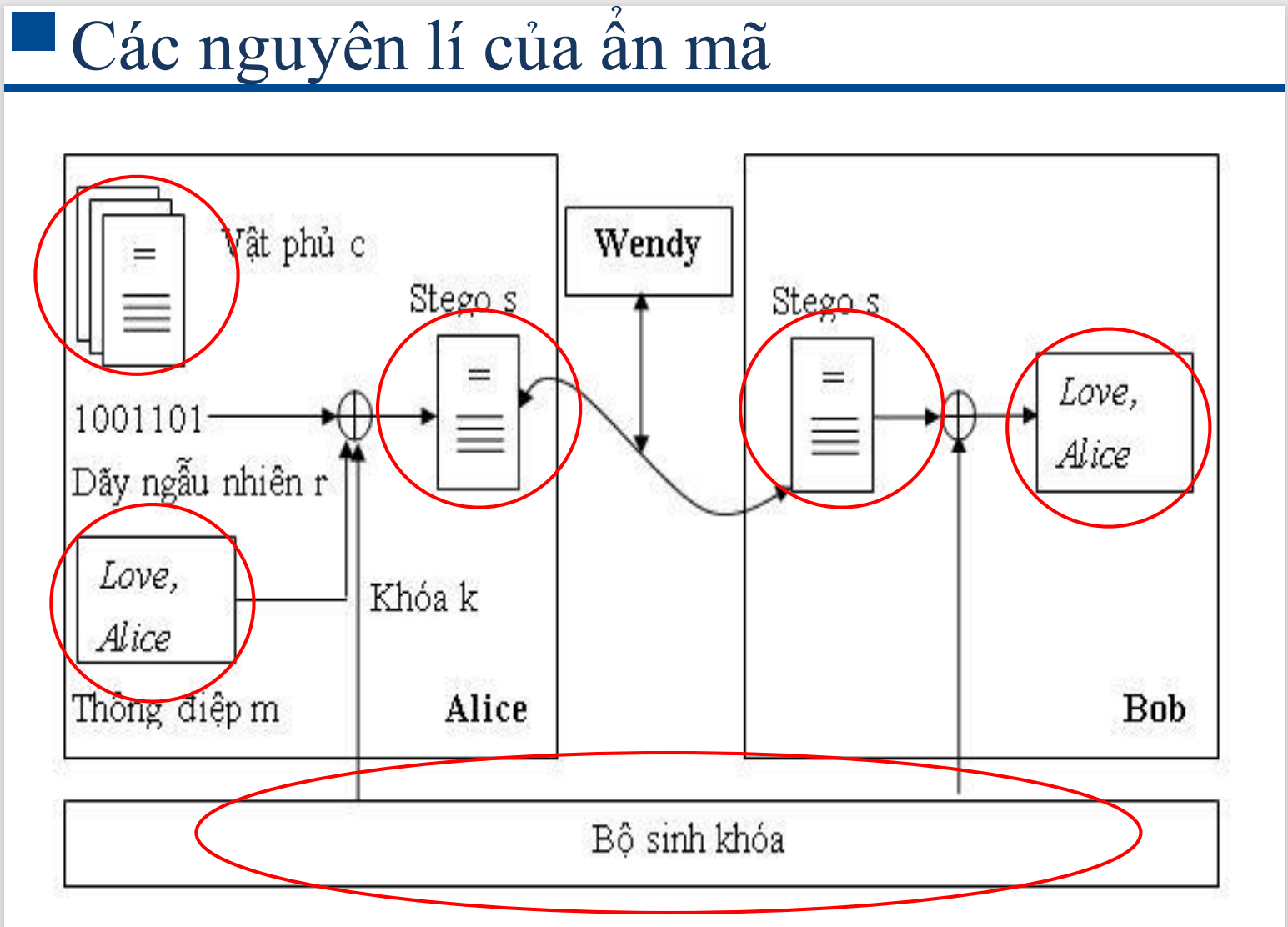
Quá trình giấu tin: Có 3 đầu vào: Môi trường chứa (audio, ảnh, video,text..), Thông tin giấu và khóa giấu tin cho vào bộ nhúng thông tin là một thuật toán giấu tin cụ thể nào đó sau khi thực hiện qua các bước giấu tin thì sẽ được đầu ra. Đầu ra đó chính là môi trường chứa đã được giấu tin rồi và sau đó sẽ chuyển đến các kênh phân phối. Quá giấu tin có thể có hoặc không tùy thuộc vào thuật toán giấu tin

-Quá trình trích xuất tin: Có 2 đầu vào là môi trường chứa đã được giấu tin và khóa giấu tin được thông qua bộ trích xuất thông tin là thuật toán đảo ngược của thuật toán nhúng được đầu ra là Thông tin giấu. Phần kiểm định thì được sử dụng để kiểm tra thủy vân xem có bị giả mạo hay không so với thủy vân ban đầu



**Câu 5: Trình bày sơ đồ về nguyên lý của ẩn mã. Giải thích ý nghĩa của dãy ngẫu nhiên lấy từ vật phủ.**

-Sơ đồ về nguyên lí của ẩn mã



Các nguyên lý

1.Thông điệp

2.Vật phủ là một tập vật phủ(VD: các bức tranh khác nhau) cho các lần khác nhau. Áp dụng bộ sinh khóa nếu trong phương pháp có sử dụng khóa

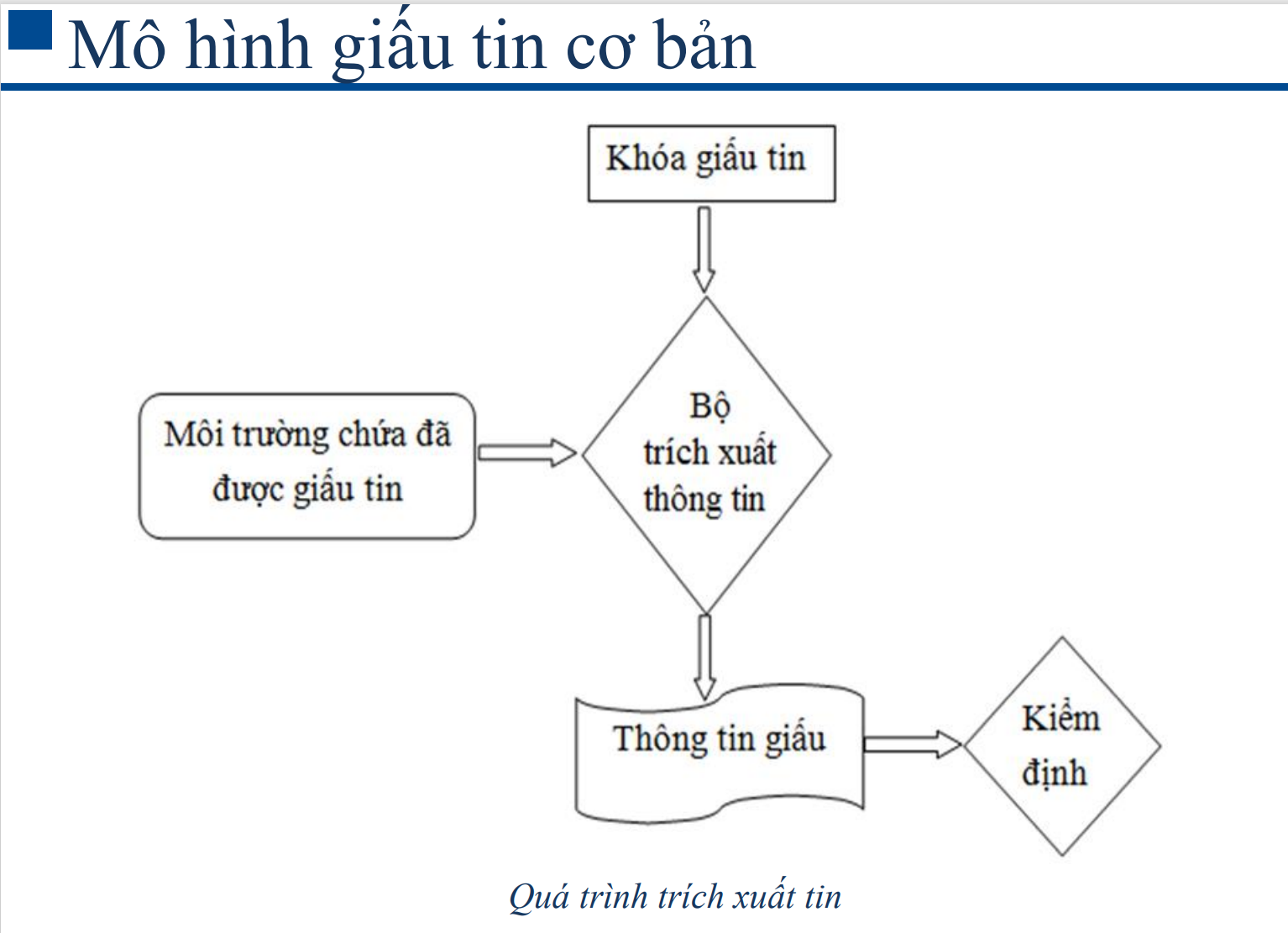
3.Thực hiện các phương pháp nhúng tạo thành vật có chứa tin

4.Truyền đi trên các kênh công khai, không an toàn, kẻ thứ 3 có thể bắt được

5. Bob nhận được stego sử dụng bộ sinh khóa trích xuất ra thông điệp: có thể là sử dụng ẩn mã thuần túy, ẩn mã khóa bí mật hoặc ẩn mã khóa công khai.

-Ý nghĩa của dãy ngẫu nhiên lấy từ vật phủ: r được lấy ra từ vật phủ một cách ngẫu nhiên. Lấy ngẫu nhiên bất kì một chuỗi nào trong vật phủ c để tăng mức độ an toàn cho việc ẩn mã. Nếu thực hiện theo phương thức lấy dãy tuần tự thì sẽ stego này sẽ rất dễ bị phá vỡ.

**Câu 6: Vẽ sơ đồ quá trình trích xuất tin. Tại sao sau khi trích xuất thông tin lại không thu được vật phủ ban đầu?**



-Khi trích xuất không thu được vật phủ vì: khi trích xuất, người nhận chỉ biết vị trí nhúng và tách thông tin đó mà không biết nội dung ban đầu của bị trí nhúng tin có bị thay đổi hay không. Nên trong thủy vân số có quá trình kiểm định để kiểm tra xem có bị giả mạo hay không so với thủy vân ban đầu

**Câu 7: Nêu khái niệm về giấu tin số. Phân biệt giấu tin và ẩn mã. Nêu một số tính chất ảnh hưởng tới quá trình giấu tin.**

-Giấu tin số là kĩ thuật nhúng một lượng thông tin số vào trong một đối tượng dữ liệu khác

-So sánh giấu tin và ẩn mã

-Một số tính chất ảnh hưởng tới quá trình giấu tin

+Sự thay đổi trên đối tượng chứa: là tối thiểu

* Không thể bị suy biến
* Đảm bảo chất lượng
* Nếu là truyền thông tin mật thì sự thay đổi phải là rất nhỏ
* Không có sự thay đổi về dung lượng

+Mức độ tránh các thao tác biến đổi trên đối tượng chứa

* Văn bản: dịch chuyển từ, chia khoảng cách giữa các từ.
* Ảnh tĩnh: các phép biến dổi affine, nhiễu, các phép biến đổi phi hình học, lọc nhiễu,…
* Mô hình ba chiều: các phép biến đổi affine, biến đổi hình học, biến đổi phi hình học,…
* Âm thanh: lọc nhiễu,…

+Số lượng dữ liệu nhúng

+Sự khó phát hiện bởi tri giác con người: Tỉ lệ nghịch với dung lượng nhúng và tính bền vững

**Câu 8: Thế nào là vật ẩn mã. Phân biệt vật ẩn mã với vật phủ. So sánh kĩ thuật ẩn mã trên miền không gian với miền tần số.**

-Vật ẩn mã là vật sau khi được ẩn mã(stego object).

-Phân biệt vật ẩn mã với vật phủ: Vật phủ là đối tượng được dùng để ẩn mã (cover object) . Vật phủ và vật ẩn mã có bề ngoài không khác nhau. Tuy nhiên thì khi tác động nhúng tin lên vật phủ thì có thể thay đổi những đặc tính thống kê của vật phủ ban đầu, có thể sử dụng nhiều phương pháp để phân tích ẩn mã. Nên có thể dựa vào điều này để phiên biệt chúng.

-So sánh kĩ thuật ẩn mã trên miền không gian với miền tần số:

|  |  |
| --- | --- |
| Miền không gian | Miền tần số |
| * Giấu tin trực tiếp vào các điểm ảnh * Dễ thực hiện, dễ cài đặt * Dung lượng nhúng nhiều hơn * Kém bền vững hơn * Kém an toàn hơn | * Giấu vào các hệ số tần số của điểm ảnh * Khó thực hiện * Dung lượng nhúng ít hơn * Bền vừng hơn * An toàn hơn |

* Ưu, nhược điểm của miền tần số
* Ưu điểm

+Giấu tin trên miền tần số ảnh hưởng tương đối bền vững

+Mọi phép biến đổi ảnh, xộng nhiễu vào ảnh sẽ không bị phá hỏng thông tin giấu

+Tin được ẩn khó bị phát hiện và khó phân tích ẩn mã

* Nhược điểm

+Dùng một số kỹ thuật xử lý ảnh số như sử dụng bộ lọc nhiễu có thể làm mất thông tin mật

+Dung lượng thông tin giấu nhỏ.

**Câu 9: Ứng dụng của giấu tin trong thực tế**

Ứng dụng của giấu tin trong thực tế:

-Giấu tin bí mật

-Bảo vệ bản quyền tác giả

-Nhận thực 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 dỗi quyền thông

**Câu 10: Nêu khái niệm kĩ thuật ẩn mã LSB. Trình bày ưu, nhược điểm của kĩ thuật ẩn mã LSB.**

-Khái niệm: LSB là bit có trọng số thấp nhất. Kĩ thuật ẩn mã LSB: là thay thế các bít có trọng số thấp nhất hay chèn thông tin cần giấu vào LSB. Khi thay đổi bit ít quan trọng của một điểm ảnh thì màu sắc của điểm ảnh mới sẽ tương đối gần với điểm ảnh cũ.

\*Ưu, nhược điểm của kĩ thuật ẩn mã LSB

-Ưu điểm: đơn giản, dễ thực hiện, chi phí thấp

-Nhược điểm: dễ bị tấn công

**Câu 11: Hãy trình bày quá trình nhúng của thuật toán giấu và tìm kiếm tuần tự(or ngẫu nhiên) bằng cách thay thế LSB trên miền không gian. Nếu yêu cầu giấu tin với tỉ lệ nhúng là p% so với kích cỡ ảnh thì thuật toán này cần thay đổi như thế nào?**

**Câu 13: Có nhận xét gì về thông điệp trích xuất theo thuật toán giấu và tìm kiếm tuần tự so với thông điệp ban đầu?**

**Câu 14: Tại sao trong thuật toán Jsteg không được nhúng tin vào các hệ số DC, AC = 0, AC = 1? Thuật toán nhúng Jsteg có an toàn hơn so với thuật toán giấu và tìm kiếm tuần tự trên LSB? Vì sao?**

-Trong thuật toán Jsteg không được nhúng tin vào các hệ số DC, AC=0 , AC=1 tại vì hệ số DC chứa giá trị trung bình của tất cả các hệ số khác trong khối, và là giá trị lớn nhất. Các hệ số DC rất quan trọng cho mỗi khối vì chúng cung cấp một ước lượng tốt cho mức độ chi tiết trong khối. Thay đổi giá trị hệ số DC sẽ gây nhiều thay đổi giá trị cho các hệ số AC. Điều này tạo ra một sự khác biệt khi hình ảnh được chuyển đổi trở lại trên miền không gian. Còn khi nhúng vào AC=0, AC=1 làm thay đổi đáng kể giá trị thống kê nên có thể bị tấn công thống kê.

-Theo em, thuật toán Jsteg không an toàn hơn so với thuật toán giấu và tìm kiếm tuần tự trên LSB .Vì thuật toán này thay vì giấu trên miền không gian thì được giấu trên miền tần số và cũng thực hiện nhúng tuần tự và không có khóa k. Trích xuất thông điệp thì cũng không cần khóa trích xuất mà chỉ cần từ ảnh stego biến sang miền tần số sau đó trích xuất tại những vị trí khác DC, AC=0, AC=1 ra được chuỗi bít thông điệp.

**Câu 15: Trình bày thuật toán Outguess. Tại sao thuật toán lại không cho phép nhúng vào hệ số DC và AC bằng 0 hoặc 1? Thuật toán này đã cải tiến gì so với thuật toán Jsteg?**

-Thuật toán Outguess đã có cải tiến hơn so với thuật toán Jsteg, ở thuật toán này đã có sử dụng khóa K để có thể hoán đổi vị trí các vị trí một cách ngẫu nhiên giúp cho quá trình ẩn tin được an toàn hơn

**Câu 16: Trong thuật toán Wulee, tại sao cần thỏa mãn điều kiện bất biến để thực hiện nhúng tin vào khối bit**

-Tại vì nếu xảy ra các trường hợp:

+ toàn bằng 0 hoặc toàn bằng 0 thì

+ toàn bằng 1 hoặc trùng với K thì

Thì nếu giấu tin vào trong trường hợp toàn bằng 0 quy định là toàn màu đen, ta giấu bit 1 quy định là màu trắng thì có thể đoán ra được cái bit tương ứng màu trắng đấy chính là bit 1 trong khóa K và sẽ dần suy đoán được khóa K và nếu suy đoán được khóa K thì sẽ dễ dàng lấy được thông tin mật được giấu trong đấy.

**Câu 16.1: Với một khối ảnh con nào đó, tại sao trong trường hợp thì phải chọn vị trí điểm ảnh có bít bằng 0 để đảo**

Vì giả sử như chọn 1 bit ngẫu nhiên thỏa mãn đồng thời và chuyển thành 0 thì => . Khi đó thì điều kiện không còn thỏa mãn.

Tương tự với câu hỏi đối với trường hợp : thì lúc này thì điều kiện không còn thỏa mãn.

**Câu 16.2: Bất biến của thuật toán Wulee là gì? Vai trò của bất biến đó thể hiện như thế nào?**

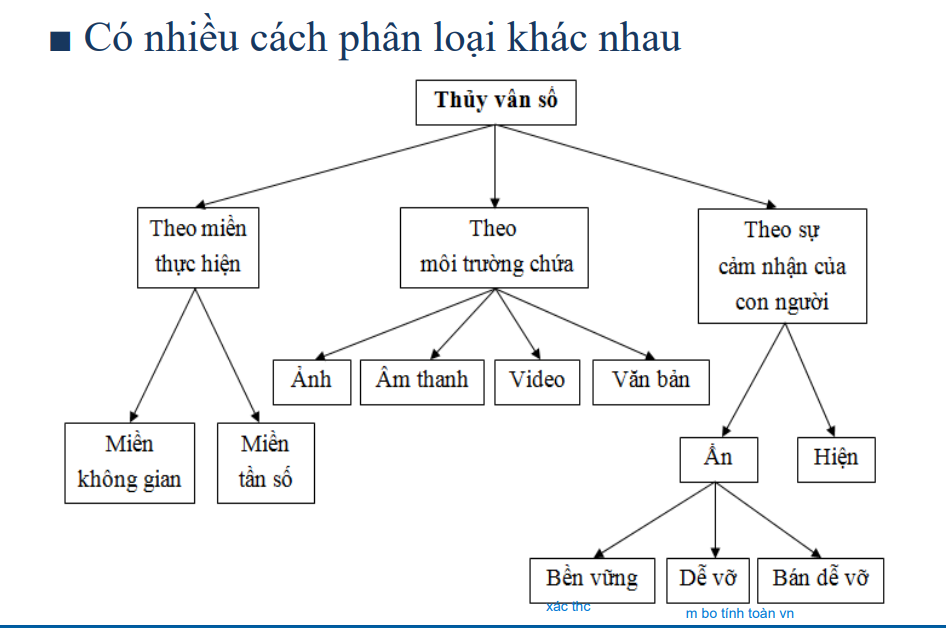
Bất biến trong Wulee là điều kiện . Bất biến này trong quá trình giấu hay trích xuất thì đều kiểm tra điều kiện nếu thỏa mãn thì chính là bít được giấu.

**Câu 17: Nêu khái niệm thủy vân. So sánh thủy vân với ẩn mã.**

-Thủy vân là quá trình nhúng dữ liệu vào một đối tượng đa phương tiện nhằm xác thực nguồn gốc hay chủ sở hữu của đối tượng đó.

-So sánh thủy vân với ẩn mã

|  |  |  |
| --- | --- | --- |
| **Tiêu chí** | **Ẩn mã** | **Thủy vân số** |
| Mục đích | Bảo vệ thông tin | Bảo vệ môi trường giấu tin |
| Dung lượng nhúng | Càng nhiều càng tốt | Đủ để đặc trung cho bản quyền của chủ sở hữu |
| Độ trong suốt | Phải ẩn | Tùy vào hệ thống |
| Chỉ tiêu quan trọng nhất | Dung lượng nhúng | Tính bền vững |

**Câu 18: Trình bày sự phân loại các kĩ thuật thủy vân. So sánh thủy vân trên miền không gian và thủy vân trên miền tần số?** ****

-So sánh thủy vân trên miền không gian và thủy vân trên miền tần số:

|  |  |  |
| --- | --- | --- |
| Nội dung | Thủy vân trên miền không gian | Thủy vân trên miền tần số |
| Ưu điểm | -Đơn giản, không cần vật phủ để trích xuất thủy vân  -Dung lượng nhúng nhiều | -Bền vững hơn thủy vân trên miền không gian trước các phép biến đổi ảnh (năng lượng của ảnh tập trung vào các thành phần có tần số thấp nên nhúng vào đó thì những biến đổi sẽ được phân phối trên toàn bộ ảnh |
| Nhược điểm | -Không bên vững đối với tấn công nén mất dữ liệu, cắt dán ảnh, thêm nhiễu bởi thủy vân bị biến dạng | -Phức tạp hơn  -Dung lượng nhúng ít hơn |

**Câu 19: Trình bày các tính chất của một hệ thống thủy vân số. Tính chất nào là quan trọng nhất? Tại sao?**

**-**Các tính chất của một hệ thống 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.

+Dung lượng nhúng là số lượng thông tin có thể được giấu trong vật phủ.

+Trong suốt: Không thể cảm nhận được bằng các giác quan thông thường của con người về thủy vân đã được nhúng.

+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.

+Chi phí tính toán: là độ phức tạp của thuật toán sử dụng trong mô hình thủy vân. Là vấn đề quan trọng đặc biệt trong các ứng dụng giám sát truyền thông do việc sản xuất đa phương tiện không được phép chậm và quá trình hiện thủy vân phải được thực hiện với thời gian thực

**Câu 20: Trình bày thuật toán thủy vân thay thế trên miền không gian. Phân biệt sự khác nhau của thủy vân khi được thay thế vào mặt phẳng bit quan trọng nhất và mặt phẳng bit ít quan trọng nhất.**

-Thuật toán:

+Lấy các điểm ảnh từ ảnh phủ

+Lấy các điểm ảnh từ thủy vân

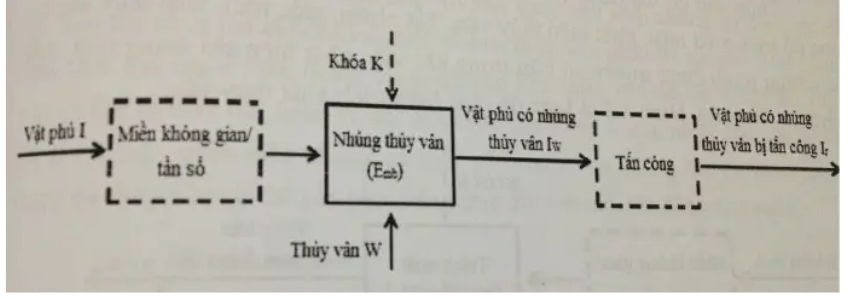
+Thay thế LSB của các điểm ảnh trong ảnh phủ bởi các bit của thủy vân

-Khi thay thế vào mặt phẳng bit quan trọng nhất thì

**Câu 21: Trình bày lược đồ phát hiện/trích xuất thủy vân, ghi rõ công thức trích xuất, phát hiện và giải thích các tham số.**

1.Nhúng thủy vân số

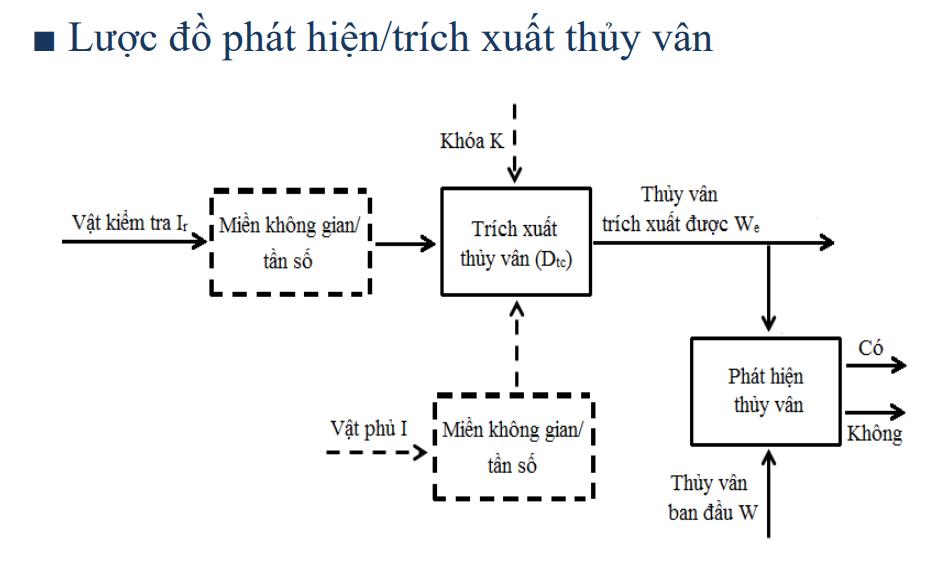
Lược đồ nhúng thủy vân



* Công thức nhúng
* Nhúng trên miền không gian
* Nhúng trên miền tần số
* Giải thích các thâm số nhúng:
* : hàm nhúng thủy vân
* : vật phủ dùng để nhúng thủy vân vào
* : thủy vân ban đầu cần nhúng
* : vật phủ sau khi được nhúng thủy vân
* : khóa sử dụng trong quá trình nhúng và phát hiện/trích xuất thủy vân (K không nhất thiết phải có mà tùy thuộc kỹ thuật, K không được sử dụng nhằm tăng tính an toàn cho hệ thống thủy vân).
* : 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

2.Trích xuất thủy vân

* Lược đồ trích xuất thủy vân



Công thức trích xuất thủy vân:

-Trích xuất thủy vân mù

-Trích xuất thủy vân không mù

-Đầu ra của quá trình phát hiện là 1 giá trị nhị phân

D(In, W, K){0: không có thủy vân, 1: có thủy vân}

-Giải thích tham số:

* Dtc: hàm trích xuất thủy vân
* D: hàm phát hiện thủy vân
* Ir: vật có nhúng thủy vân nhưng đã bị tấn công trên đường truyền, cũng là vật dùng để kiểm tra trong quá trình phát hiện/trích xuất thủy vân.
* I: vật phủ dùng để nhúng thủy vân vào
* W: thủy vân ban đầu cần nhúng
* K: khóa sử dụng trong quá trình nhúng và phát hiện/trích xuất thủy vân(K không nhất thiết phải có mà tủy kỹ thuật, K được sử dụng nhằm tăng tính an toàn cho hệ thống thủy vân).

**Câu 22: Trình bày thuật toán thủy vân dựa trên phương pháp thay thế LSB trên miền không gian**

-Đưa ra một số giả thiết sau:

* H là ảnh phủ xám có kích thước N x M
* W là ảnh thủy vân nhị phân kích thước M x M
* L là số bit được sử dụng trong mức xám của các điểm ảnh
* XOR là phép toán thay thế các bit của thủy vân vào các LSB của ảnh phủ

-Thuật toán:

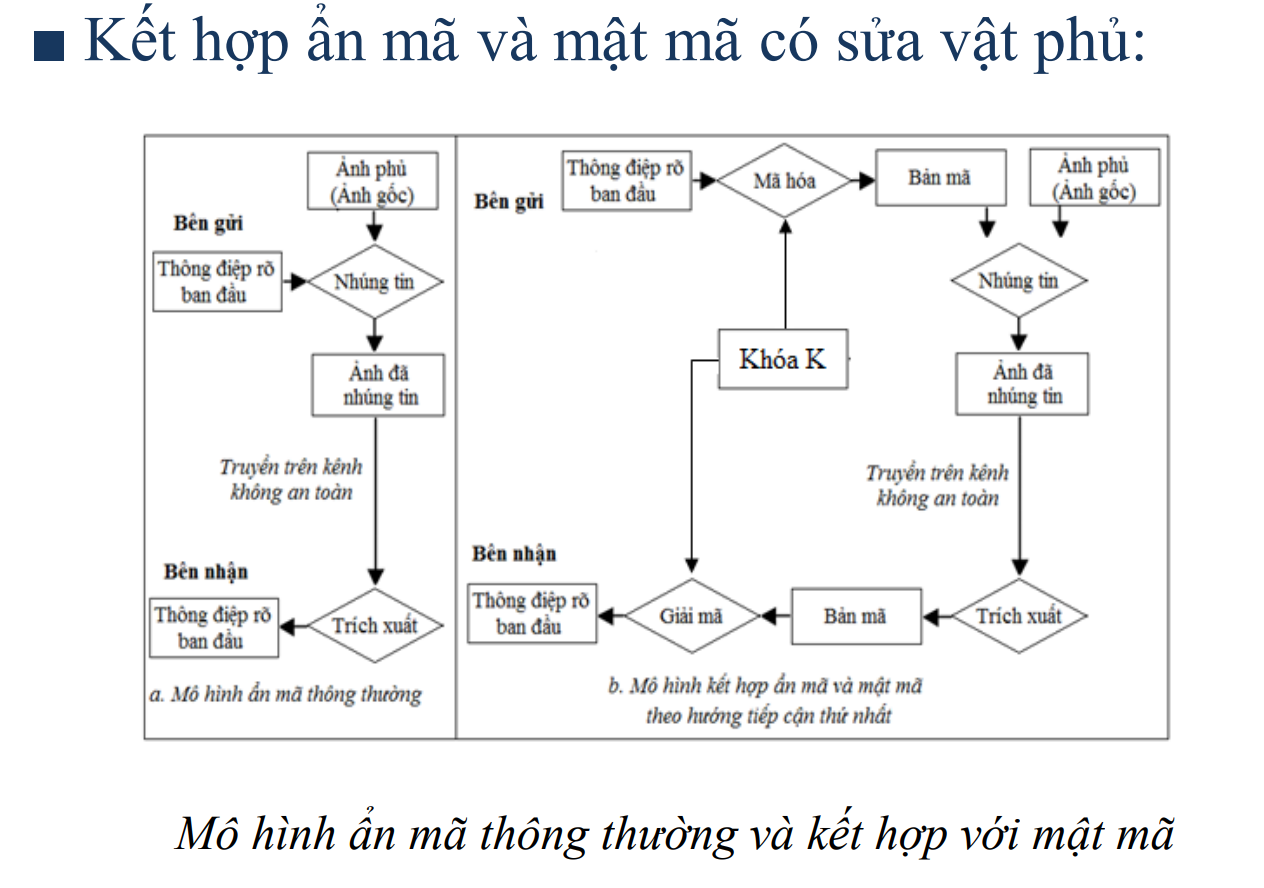
+Lấy các điểm ảnh từ ảnh phủ

+Lấy các điểm ảnh từ thủy vân

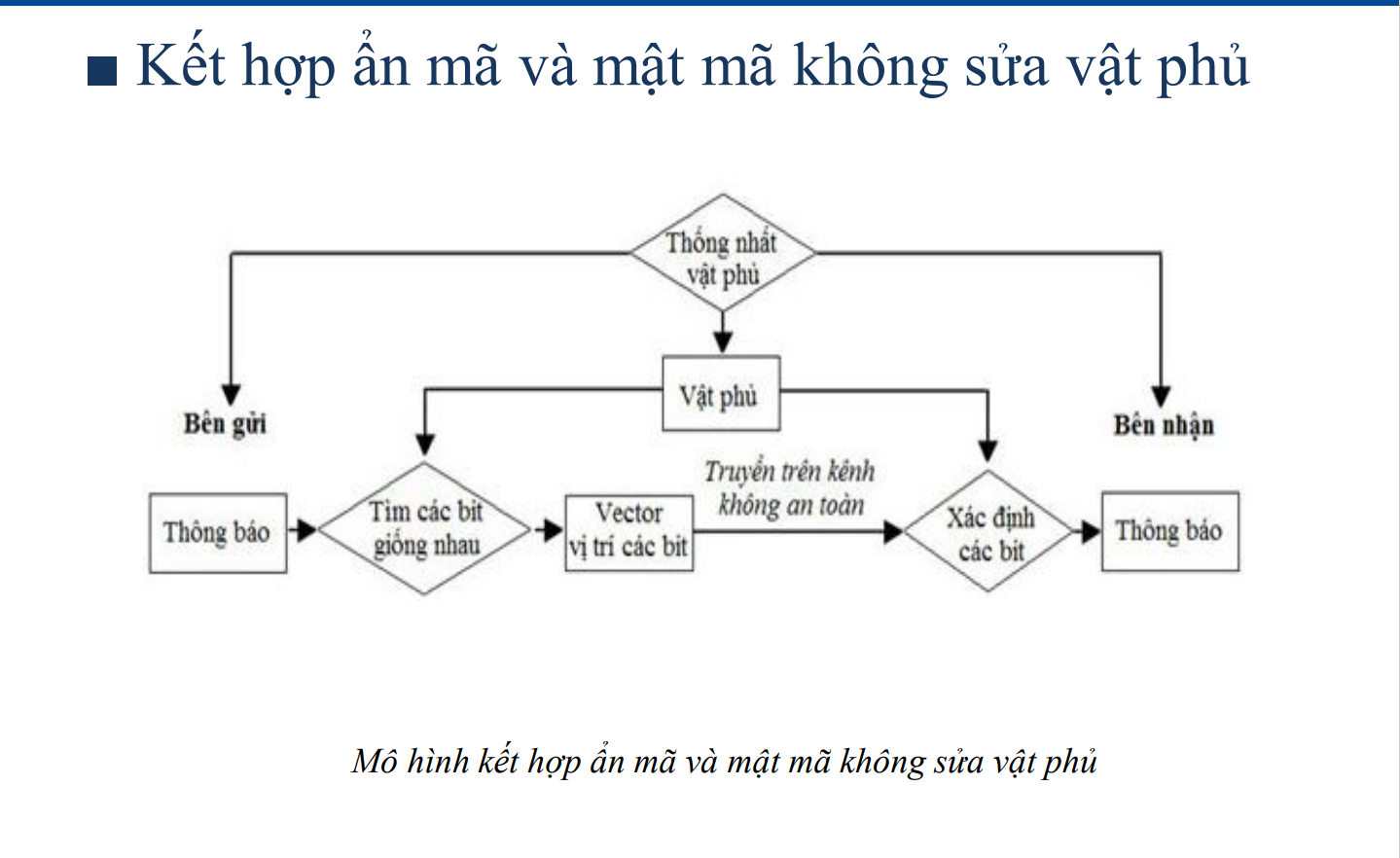
+Thay thế LSB của các điểm ảnh trong ảnh phủ bởi các bit của thủy vân

**Câu 23: Mô hình kết hợp ẩn mã và mật mã có sửa vật phủ và không sửa vật phủ**

-Có sửa vật phủ



-Không sửa vật phủ



**Câu 24: Cấu trúc của hệ thống thủy vân số**

