MỤC LỤC

Contents

[**1-** **Nêu khái niệm giấu tin số, trình bày tóm tắt mô hình phân loại giấu tin theo khuynh hướng.** 1](#_Toc486714789)

[**2- Các ứng dụng của giấu tin trong thực tế** 1](#_Toc486714790)

[**3-** **Trình bày mô hình và tóm tắt nguyên lý ẩn mã** 3](#_Toc486714791)

[**4-** **Tóm tắt Quá trình xử lý ảnh nén jpeg(7 bước)** 5](#_Toc486714792)

[**6-** **Sự khác biệt giữa kỹ thuật nhúng trên miền không gian với trên miền tần số, nêu ưu nhược của miền tần số** 7](#_Toc486714793)

[**7-** **Tại sao trong thuật toán Jstec ta không được nhúng tin vào các hệ số DC, AC=0 hoặc AC=1. Thuật toán Jstec có an toàn hơn so với thuật toán giấu và tìm kiếm tuần tự trên LSB hay không, why?** 8](#_Toc486714794)

[**8-** **Vẽ và trình bày mô hình kết hợp ẩn mã và mật mã có sửa vật phủ và không sửa vật phủ** 8](#_Toc486714795)

[**9-** **Trình bày về phân tích ẩn mã dựa trên điều tra số** 9](#_Toc486714796)

[**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** 10](#_Toc486714797)

[**12.Nêu khái niệm, ý nghĩa của thủy vân số** 10](#_Toc486714798)

[**13.So sánh ẩn mã và thủy vân số** 11](#_Toc486714799)

[**14.Sự phân loại thủy vân và sự tóm tắt từng loại** 11](#_Toc486714800)

[**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** 12](#_Toc486714801)

[**16.Trình bày lược đồ nhúng và trích xuất thủy vân, ghi rõ công thực nhúng, trích xuất và giải thích các tham số** 13](#_Toc486714802)

[**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** 15](#_Toc486714803)

[**18.So sánh thủy vân trên miền không gian, miền tần số** 16](#_Toc486714804)

[**19.Trình bày thuật toán thủy vân dựa trên phương pháp thay thế LSB trên miền không gian.** 16](#_Toc486714805)

[**20.Trình bày phương pháp thủy vân dựa trên phép cộng trên miền không gian** 17](#_Toc486714806)

[**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.** 17](#_Toc486714807)

[**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** 18](#_Toc486714808)

[**24.Trình bày thuật toán kết hợp thủy vân trong miền không gian tần số,** 19](#_Toc486714809)

[**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:** 20](#_Toc486714810)

1. ***Nêu khái niệm giấu tin số, trình bày tóm tắt mô hình phân loại giấu tin theo khuynh hướng.***

Khái niệm:

Giấu tin là nghệ thuật “nhúng” một mẩu tin vào một vật mang tin khác.

Giấu thông tin số là kỹ thuật nhúng (giấu) một lượng thông tin số nào đó vào trong một đối tượng dữ liệu số khác.

Mục đích:

Bảo mật cho dữ liệu được giấu.

Bảo vệ cho chính đối tượng mang tin giấu.

Mô hình:

(Giau thông tin )

thủy vân số

Ân mã

Phân loại:

Ẩn mã (steganography): là kỹ thuật nhúng tin mật vào môi trường giấu tin.

Thủy vân số (watermaking): là kỹ thuật nhúng dấu ấn số vào một tài liệu hoặc sản phẩm nhằm chúng thực nguồn gốc hay chủ sở hữu.

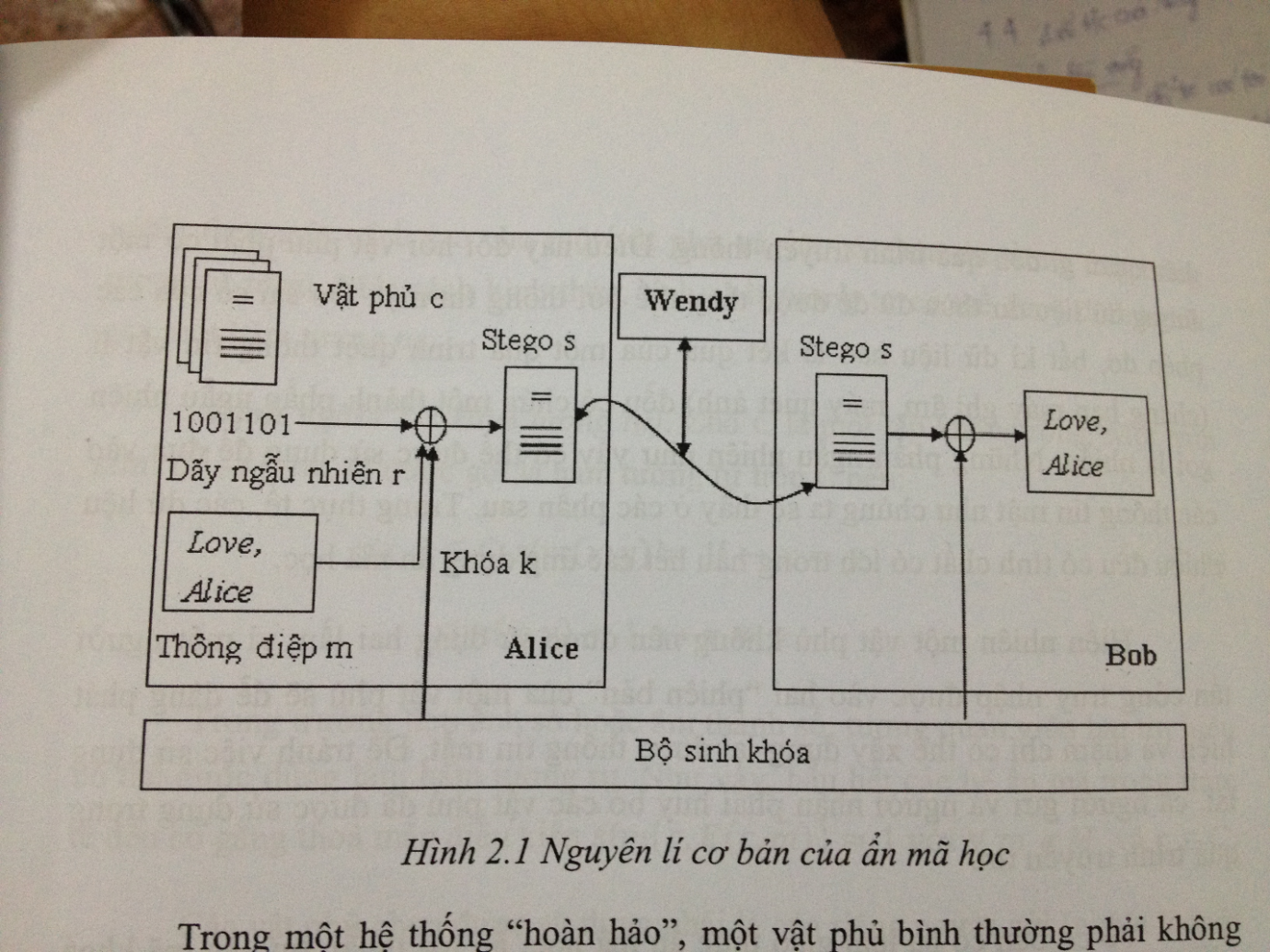
1. ***Các ứng dụng của giấu tin trong thực tế***

Một số ứng dụng của giấu tin trong thực tế như bảo vệ bản quyền ,xác thực ,truyền thông tin bí mật …

* **Bảo vệ bản quyền tác giả** (copyright protection)  
  Một thông tin nào đó mang ý nghĩa xác định quyền sở hữu của tác giả (người ta gọi nó là thuỷ vân) sẽ được nhúng vào các sản phẩm dữ liệu đa phương tiện và chỉ duy nhất người chủ sở hữu hợp pháp các sản phẩm đó có thủy vân và được dùng làm minh chứng cho bản quyền sản phẩm. Giả sư, có một thành phẩm dữ liệu dạng đa phương tiện như ảnh, âm thanh, video cần được lưu trên mạng. Việc bảo vệ các sản phẩm chống lại các hành vi lấy cắp hoặc làm nhái cần phải có một kỹ thuật để dán tem bản quyền vào sản phẩm này. Việc dán tem chính là việc “nhúng” thuỷ vân, cần phải đảm bảo không để lại một ảnh hưởng lớn nào đến việc cảm nhận sản phẩm. Yêu cầu kỹ thuật đối với ứng dụng này là thuỷ vân phải tồn tại bền vững cùng với sản phẩm, muốn hủy bỏ thuỷ vân này mà không được phép của người chủ sở hữu thì chỉ có cách là phá huỷ sản phẩm.  
  - **Xác thực thông tin hay phát hiện xuyên tạc thông tin** (authentication and tamper detection)  
  Một tập các thông tin sẽ được giấu trong phương tiện chứa sau đó được sử dụng để nhận biết xem dữ liệu trên phương tiện gốc đó có bị thay đổi hay không. Các thuỷ vân nên được “ẩn” để tránh sự tò mò của đối phương. Hơn nữa, việc làm giả các thuỷ vân hợp lệ hay xuyên tạc thông tin nguồn cũng cần được xem xét. Trong các ứng dụng thực tế, người ta mong muốn tìm được vị trí bị xuyên tạc cũng như phân biệt được các thay đổi (ví như phân biệt xem một đối tượng đa phương tiện chứa giấu thông tin đã bị thay đổi, xuyên tạc nội dung hay chỉ là bị nén mất dữ liệu). Yêu cầu chung đối với dữ liệu này là khả năng giấu được nhiều thông tin  và thuỷ vân không cần bền vững trước các phép xử lvý trên các đối tượng đã được giấu tin.  
  **-  Giấu vân tay hay dán nhãn** (fingeprinting and labeling)  
  Thuỷ vân được sử dụng để nhận diện người gửi hay người nhận của một thông tin nào đó trong ứng dụng phân phối sản phẩm. Thuỷ vân trong trường hợp này cũng tương tự như số serial của sản phẩm phần mềm. Mỗi một sản phẩm sẽ mang một thuỷ vân riêng. Ví dụ như các thủy vân khác nhau sẽ được nhúng vào các bản copy khác nhau của thông tin gốc trước khi chuyển cho người nhận. Với những ứng dụng này thì yêu cầu đảm bảo độ an toàn cao cho các thuỷ vân tránh sự xoá dấu vết trong khi phân phối.  
  **-  Kiểm soát sao chép** (copy control)  
  Điều mong muốn đối với các hệ thống phân phối dữ liệu đa phương tiện là tồn tại một kỹ thuật chống sao chép trái phép dữ liệu. Có thể sử dụng thuỷ vân để chỉ trạng thái sao chép của dữ liệu. Các thuỷ vân trong trường hợp này được sử dụng để kiểm soát sao chép đối với các thông tin. Các thiết bị phát hiện ra thuỷ vân  thường được gắn sẵn vào trong các hệ thống đọc - ghi. Ví dụ như hệ thống quản lý sao chép DVD đã được ứng dụng ở Nhật. Thuỷ vân mang các giá trị chỉ trạng thái cho phép sao chép dữ liệu như “không được sao chép” (copy never) hay “chỉ được sao chép một lần” (copy once), sau khi copy xong, bộ đọc -  ghi thuỷ vân sẽ ghi thuỷ vân mới chỉ trạng thái mới lên DVD. Các ứng dụng loại này cũng yêu cầu thuỷ vân phải được đảm bảo an toàn và cũng sử dụng được phương pháp phát hiện thuỷ vân đã giấu mà không cần thông tin gốc.  
  **-  Giấu tin mật** (steganography)  
  Các thông tin có thể giấu được trong những trường hợp này càng nhiều càng tốt sao cho vẫn đảm bảo yêu cầu là không thể phát hiện được. Việc giải mã để lấy được thông tin cũng không cần phương tiện mang gốc ban đầu. Các yêu cầu về chống tấn công của đối phương không cần cao lắm, thay vào đó là yêu cầu thông tin giấu phải được bảo mật.  
  Kỹ thuật giấu thông tin đang được áp dụng cho nhiều loại đối tượng chứ không riêng gì dữ liệu đa phương tiện như ảnh, audio, video. Gần đây, đã có một số nghiên cứu giấu tin trong cơ sở dữ liệu quan hệ.

1. ***Trình bày mô hình và tóm tắt nguyên lý ẩn mã***

Mô hình



Các nguyên lý

1 Thông điệp.

2 vật phủ là một tập vật phủ(ví dụ các bức ảnh 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

* 1. Ẩn mã thuần túy: là hệ ẩn mã trong đó không yêu cầu trao đổi các thông tin mật về khóa.
     + Bộ bốn = (C, M, D, E). Trong đó:
       - C: tập các vật phủ có thể.
       - M: tập các thông điệp có thể, với |C| >= |M|.
       - E: C x M -> C là hàm nhúng thông tin vào.
       - D: C -> M là hàm trích xuất thông tin với tính chất:

D (E (c, m)) = m, với mọi m M và c C.

* 1. Ẩn mã khóa bí mật: tương tự hệ mật mã khóa đối xứng.
     + Bộ năm = (C, M, K, Dk, Ek). Trong đó:
       - C: tập các vật phủ có thể:
       - M: tập các thông điệp có thể: |C| >= |M|.
       - K: tập các khóa bí mật.
       - Hàm nhúng Ek: C x M x K -> C.
       - Hàm trích xuất Dk: C x K -> M với tính chất:

Dk (Ek (c, m, k) = với mọi m M và c C được gọi là hệ ẩn mã hóa bí mật.

* 1. Ẩn mã khóa công khai
     + Sử dụng hai khóa: khóa công khai trong quá trình nhúng, khóa bí mật trong quá trình trích xuất.
     + Sử dụng hệ mật mã khóa công khai.

1. ***Tóm tắt Quá trình xử lý ảnh nén jpeg(7 bước)***

Qúa trình xử lý ảnh nén JPEG

B1 :Chuyển đổi điểm ảnh 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

B2 : Giarm giá trị thành phần màu :Mục đích giảm kích cỡ ảnh

Mắt người thường nhạy cảm với những thay đổi về độ sáng hơn là những thay đổi về màu sắc =>giảm kích cỡ tổng thể của tệp thường sử dụng cách giảm chất lượng màu .

Nén ảnh JPEG thường giảm chất lượng màu bằng cách lấy 4 điểm ảnh lân cận và lấy giá trị trung bình của chúng ,việc này cho toàn bộ ảnh mất đi 1 lượng thông tin của hình ảnh ,tức là chiếm khoảng nửa .Tuy nhiên sẽ không có bất cứ điều gì gây chú ý về chất lượng của hình ảnh ở đây .

B3 : Chuyển các giá trị điểm ảnh sang tần số

-Phép biến đổi Fourier(DFT),cosin rời rạc (DCT) đuêọc sử dụng để ánh xạ 1 tín hiệu vào miền tần số .

-DCT biến đổi dữ liệu dưới dạng biên độ thành dữ liệu dưới dạng tần số

-DCT đã trở thành tiêu chuẩn quốc tế cho các hệ thống mã chuyển vị bởi nó có đặc tính gói năng lượng tốt ,cho kết quả là số thực và có các thuật toán nhanh để hiện chúng

-DCT gồm :DCT 1 chiều

DCT 2 chiều

B4 :Lượng tử hóa

Bước quan trọng nhất khi nén ảnh JPEG

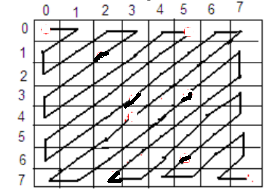
-Mục đích là để lượng tử các giá trị biểu thị cho hình ảnh sau giai đoạn chuyển đổi giá trị điểm ảnh snag tần số .

-Sau quá trình này 1 lượng lướn dữ liệu có thể được loại bỏ mà k ảnh hưởng tới chất lượng ảnh

-Cần phải xác định là trong quá trình lượng tử hóa có trọng số có xảy ra mất thông tin,gây tổn hao.Đây là bước tổn hao duy nhất trong thuật toán nén .

B5 : sắp xếp zic zac

Việc lượng tử các hệ số DCT ở trên khá là điển hình .Chỉ có 1 vài giá trị được giữ lại là khác không đa số sẽ luôn luôn là số 0 .Thường thì các số khác không luôn nằm ở phía bên trên bên trái và các số không ở góc dưới bên phải .Trong giai đoạn nén JPEG các giá trị này được sắp xếp lại bằng cách dùng một loại chuyển động “zic zắc “ để các tần số tương tự được nhóm lại với nhau .Việc xử lý 64 hệ số của khối 8\*8 pixel bằng cách quét zig-zag làm tăng tối đã chuỗi các giá trị 0 và o vậy tăng hiệu quả nén.



Hình :sắp xếp zic zac của các thành phần ảnh JPEG

B6 :Mã hóa độ dài chạy (RLC )

-Thành phần AC sau khi quét ziczac thì các giá trị 0 giống nhau sẽ được thay thế bằng mã RLC

-Dấu EOB :đánh dấu vị trí bắt đầu của chuỗi các số 0 liên tiếp

B7 :Mã hóa độ dài thay đổi VLC

Mã hóa thành phần DC :Gía 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 (# DC )

1. Cách thực hiện giấu tin mật trên LSB theo tỉ lệ P% so với kích cỡ ảnh(giấu ngẫu nhiên hoặc giấu tuần tự)
2. ***Sự khác biệt giữa kỹ thuật nhúng trên miền không gian với trên miền tần số, nêu ưu nhược của miền tần số***

* **So sánh**

|  |  |
| --- | --- |
| 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 tương đối bền vững

+ mọi phép biến đổi ảnh, cộng nhiễu vào ảnh sẽ không phá hỏng tin giấu

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

* Nhược điểm

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

+ Dung lượng thông tin giấu nhỏ

1. ***Tại sao trong thuật toán Jstec ta không được nhúng tin vào các hệ số DC, AC=0 hoặc AC=1. Thuật toán Jstec có an toàn hơn so với thuật toán giấu và tìm kiếm tuần tự trên LSB hay không, why?***

* **Thuật toán Jeteg không nhúng tin vào các hệ số DC, AC=0 hoặc AC=1**

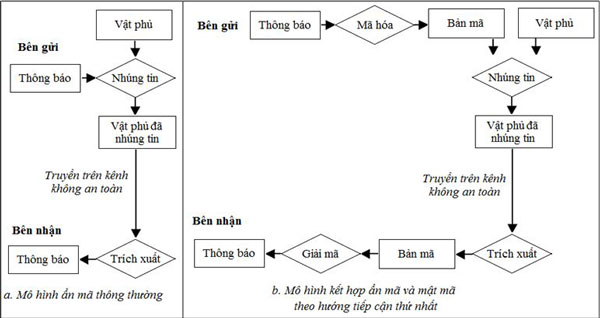
Hệ số AC chứa các giá trị trung bình của tất cả các hệ số khác trong khối. Các hệ số DC rất là quan trọng cho mỗi khối vì chúng cung cấp cho một ước lượng tốt như mức độ chi tiết trong khối. Thay đổi giá trị hệ só DC cũng sẽ thay đổi nhiều giá trị của các hệ số AC, và điều này sẽ tạo ra một sự khác biệt khi hình ảnh được chuyển đổi trở lại tên miền không gian và được xem bình thường. Vì lí do này, thuật toán Jsteg không nhúng thông điệp dữ liệu trên bất kỳ các hệ số DC cho mỗi khối. Thêm vào đó, thuật toán cũng không cho phép nhúng trên bất kỳ hệ số AC=1 và =0.

* **Thuật toán Jsteg có an toàn hơn so với thuật toán giấu và tìm kiếm tuần tự trên LSB hay không, tại sao?**

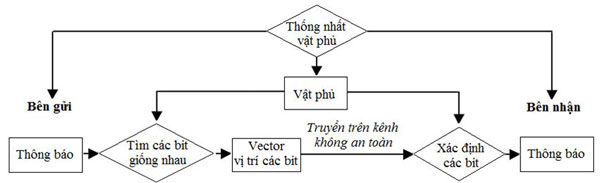
Thuật toán Jsteg có an toàn hơn so với thuật toán giấu và tìm kiếm tuấn tự trên LSB. Vì cả 2 thuật toán đều không dùng khóa, nhưng sự an toàn của Jsteg nằm trong thuật toán

1. ***Vẽ và trình bày mô hình kết hợp ẩn mã và mật mã có sửa vật phủ và không sửa vật phủ***

**Mô hình kết hợp ẩn mã và mật mã có sửa vật phủ**



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



* Độ an toàn phụ thuộc

+ Vật phủ bí mật

+ Vector vị trí các bit

1. ***Trình bày về phân tích ẩn mã dựa trên điều tra số***

* Người phân tích có thể xác định được thời điểm bên gửi, bên nhận trao đổi thông điệp bí mật
* Thực hiện chặn những thông tin bí mật
* Phân tích để đọc được nội dung thông điệp hoặc xác định được nội dung liên quan
* Người phân tích cố gắng khôi phục lại một số thuộc tính của thông điệp được nhúng và tính chất thuật toán ẩn mã
* Dựa trên thông tin có sẵn hoặc thu thập được người phân tích có thể thực hiện các kiểu tấn công khác nhau

# ***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 phân tích ẩn mã : phân tích ẩn mã thực hiện tìm kiếm để phát hiện các thông điệp được giấu trong vật phủ
* So sánh kỹ thuật phân tích mù và kỹ thuật phân tích có chủ đích

|  |  |
| --- | --- |
| Kỹ thuật phân tích có chủ đích | Kỹ thuật phân tích mù |
| - Biết thông tin ẩn mã 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 thông tin nhúng | - Không biết thuật toán ẩn mã đươc sử dụng  - Lựa chọn các đặc trưng để phân tích  - Huấn luyện bộ phân loại phân tích ẩn mã mù chỉ sử dụng ảnh phủ |

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

# ***12.Nêu khái niệm, ý nghĩa của thủy vân số***

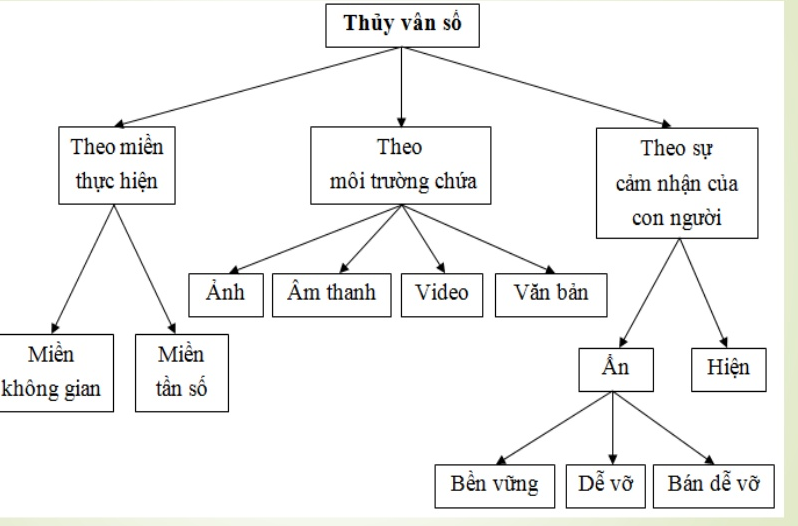
Thủy vân số là quá trình nhúng dữ liệu vào 1 đối tượng đa phương tiện nhằm xác thực nguồn gốc hay chủ sở hữu của đối tượng đó.

Ý nghĩa:

# ***13.So sánh ẩn mã và thủy vân 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 tầng số thấp nên nhúng vào đó thì những biến đổi sẽ được phân phối trên toàn bộ ảnh. |
| Nhược điểm | * Không bền vững để chống lại phép xử lý ảnh (thủy vân không được phân phối trên toàn bộ ảnh). | * Phức tạp hơn. * Dung lượng nhúng nhiều. |

# ***14.Sự phân loại thủy vân và sự tóm tắt từng loại***



Dựa theo miền thực hiện người ta chia thủy vân thành 2 loại :

* Thủy vân trên miền không gian: Là thủy vân thực hiện nhúng trực tiếp vào các giá trị vật phủ.
* Thủy vân trên miền tần số:là thủy vân mà thực hiện nhúng vào các hệ số tần số tương ứng của các giá trị của vật phủ, tức là khi nhúng cần biến đổi các giá trị vật phủ sang miền tần số thông qua các phép biến đổi chẳng hạn như DCT,DWT,…

Dựa theo mối trường chưa: thủy vân có thể chia thành các phần:

* Thủy vân trong ảnh.
* Thủy vân trong âm thanh
* Thủy vân trong video
* Thủy vân trong văn bản.

Dựa theo sự cảm nhận của con người, thủy vân được chia thành các loại:

* Thủy vân ẩn :là thủy vân sau khi được nhúng vật phủ chúng ta không thể nhìn thấy cũng như không cảm nhận được sự thay đổi của vật phủ chứa thủy vân so với vật phủ ban đầu,tuy nhiên chúng ta vẫn có thể trích xuất nó bằng cách sử dụng thuật toán thích hợp.
* Thủy vân hiện: là loại thủy vân sau khi nhúng vào vật phủ chúng ta hoàn toàn có thể nhìn thấy or cảm nhận được

Thủy vân ẩn , người ta chia thủy vân thành các loại dưới đây:

* Thủy vân bền vững: là thủy vân đc nhúng theo cách dù thay đổi 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.
* Thủy vân dễ vỡ: Là thủy vân mà bất kì một thao tác thay đổi hay sữa chữa nào cũng sẽ làm hỏng hoặc làm biến đổi thủy vân, tức là nó không chịu được bất kì tác động or tấn công nào.
* Thủy vân bán dễ vỡ: Là loại thuyt vân có thể chịu được một số phép biến đổi hợp pháp or 1 số loại tấn công nào đó chứ không phả tất cả các phép biến đổi hay mọi loại tấn công.

# ***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 đó là nhúng thủy vân và phát hiện/ trích xuất thủy vân. Trước khi mô tả chi tiết quá trình nhúng và phát hiện/trích xuất thủy vân chúng ta đửaa 1 số kí hiệu sau:

Kí hiệu:

I : Vật phủ dùng để nhúng thủy vân vào

W: thủy vân ban đầu cần nhúng.

Thủy vân trích xuất được

:vật phủ sau khi được nhúng thủy vân

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

:Hàm nhúng thủy vân

:Hàm trích xuất thủy vân

:Vật có nhúng thủy vân nhưng đac bị tấn công trên đường truyền.Cúng là vật dùng để ktra trong quá trình phát hiện trích xuất thủy vân

F(i)Hàm biến đổi vật phỉ I sang miền tần số . giá trị của f là một vector các hệ số tương ứng của vật phủ trên miền biến đổi..

-Gồm 2 quá trình:

Nhúng thủy vân

Phát hiên/trích xuất thủy vân

# ***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 thủy vân*

*Khóa K*

Tân công

Nhúng thủy vân Emb

Miền ko gian tần số

*Vật phủàà à àVật phủ có nhúng thủy vân*

*Vật phủ có nhúng thủy vân bị tấn công*

Nhúng thủy vân trên miền không gian

+Nhúng thủy vân trên miền tần số:

* Giải thích các tham số nhúng.
  + Emb: hàm (thuật toán) nhúng thủy vân.
  + I: vật phủ dùng để nhúng thủy vân vào.
  + W: thủy vân ban đầu cần nhúng.
  + IW: vật phủ sau khi được nhúng thủy vân.
  + K: khóa sử dụng trong quá trình nhúng và phát hiện/trích xuất thủy vân (K không nhất thiết phải có mà tùy kỹ thuật, K được sử dụng nhằm tăng tính an toàn cho hệ thống thủy vân).
  + f(I): 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.

*Lượ đồ trích xuất thủy vân:*

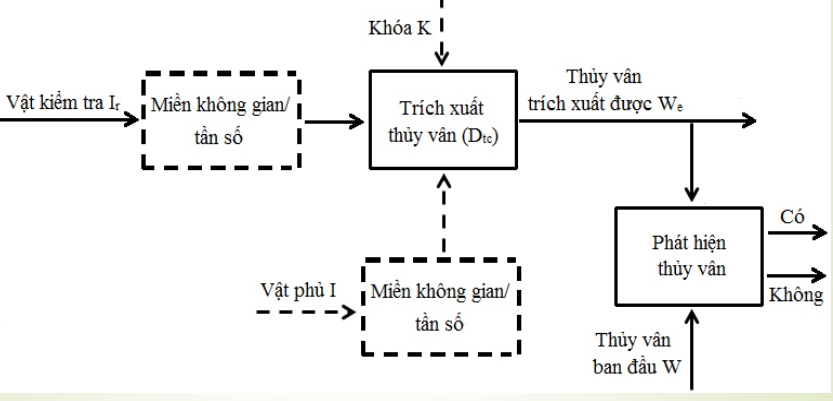
Qua trình nhúng sử dụng khóa K thì QT phát hiện/trích xuất dùng ADK.

Thủy vân mù:

Thủy vân không mù:

Qúa trình phát hiện mù sinh ra đầu ra là 1 giá trị nhị phân thể hiện sự có mặt hay ko của thủy vân W và có thể được biểu diễn như sau:

* Giải thích tham số.
* Dtc: hàm (thuật toán) 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 tùy kỹ thuật, K được sử dụng nhằm tăng tính an toàn cho hệ thống thủy vân).

**

# ***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 bền vững:*

+ Không bị thay đổi trước các tác động vật lý cũng như các tấn công

+Thường áp dụng trong trường hợp bảo về bản quyền chứ ko phù hớp với việc xác thực tính toàn vẹn của dữ liệu

*Dung lượng nhúng:*

+Là lượng thông tin có thể giấu trong vật phủ.

+luôn phải xem xét tới 2 yêu cầu quan trọng đó là tính trong suốt và tính bề vững.

* Để có được dung lượng nhúng lớn thường phải mất đi or tính bền cũng or tính trong suốt or cả hai.

*Trong suốt:*

+Không thể cảm nhận được bằng giác quan thông thường của con người về thủy vân đac được nhúng.

+ Chỉ áp dụng cho thủy vân ẩn chứ không phải thủy vân hiện

*Tính an toàn và bảo mật:*

*Chi phí tính toán:*

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

* Thủy vân trên miền không gian: Là thủy vân thực hiện nhúng trực tiếp vào các giá trị vật phủ.
* Thủy vân trên miền tần số:là thủy vân mà thực hiện nhúng vào các hệ số tần số tương ứng của các giá trị của vật phủ, tức là khi nhúng cần biến đổi các giá trị vật phủ sang miền tần số thông qua các phép biến đổi chẳng hạn như DCT,DWT,…
* Thủy vân trên miền tần số:Điểm anh được chuyển sang miền không gian hoặc tần số qua các phép biến đổi :
* Fourier rời rạc
* Cosire rời rạc.
* Sóng rời rạc

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

Trước tiên chúng ta đưa ra 1 số giả thuyết sau:

H: ảnh phủ mức xám có kích thước Nx N

W: Anh thủy vân nhị phân có kích thước MxM

L: là số bit đc sử dụng trong mức xám của điểm ảnh.

XOR là 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)

1. Lấy các điểm ảnh từ thuỷ vân.

W=

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

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

Khác với phương pháp thay thế, phương pháp thủy vân cộng ko xét những bit cụ thẻ của 1 điểm ảnh, Thay vào đó ,pp này thực hiện cộng 1 lượng giá trị thủy vân vào một điểm ảnh trong qua trình nhúng. Chúng ta có thể nhúng W vào H để thành ảnh có thủy vân như sau:

Trong đó a(i,j) là hệ số tỉ lệ.

Đối với phương pháp cộng trên miền không gian, khi trích xuất thủy vân bên nhận phải sử dụng ảnh tham chiếm(hay ảnh gốc). Lý do là 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***

# ***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.***

* Về cơ bản thì giống với trong miền không gian
* Thuật toán:
* Cho Hm và Wn tương ứng là các ảnh được chia nhỏ ra từ ảnh phủ H x N và thủy vân W cỡ M x M
* Hm-DCT là ảnh sau khi biến đổi Hm bởi phép DCT
* Hm-F là ảnh sau khi nhúng Wn  vào Hm-DCT
* Thuật toán:
* Chia ảnh phủ thành các khối ảnh có kích thước 8 x 8

H = { h(i,j), 0≤i, j < N}

Hm = { hm(i, j), 0≤ i, j< 8}

Trong đó: hm(i, j) thuộc { 0,1,2,..,2L-1}, và m là tổng số các khối 8x8

* Chia ảnh thủy vân thành các khối ảnh có kích thước 2x2

W = {w(i,j), 0≤i, j<M}

Wn = { wn(i, j), 0≤ i, j< 2}

Trong đó: Wn(i,j) thuộc {0,1}, n là tổng số khối 2x2

* Sử dụng công thức DCT để chuyển Hm thành Hm-DCT
* Chèn Wm vào các hệ số của Hm-DCT

Hm-F= {hm-F(i,j) Wm(i,j), 0≤ i, j< 8}

* Áp dụng phép biến đổi DCT ngược để chuyển ảnh có chứa thủy vân Hm-F về dạng ảnh thông thường

# ***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 trêm miền không gian chỉ đơn gainr là chèn thủy vân bằng cách thay đổi các mức xám của 1 số điểm ảnh trong ảnh phủ, tuy nhiên phương pháp này ko bền vững đối với các tấn công. Đối với thủy vân trên miền tần số thì chúng lại chèn thủy vân vào các hệ số của ảnh để biế đổi thông qua phép biến đổi DCT,DFT hay DWT. Nhìn chung, phương pháo thủy vân trong miền tần số bền vững đối với các tấn công nhưng lại ko nhúng được nhiều thông tin chất lượng ảnh sẽ bị giảm đáng kể sau khi thực hiện chèn thủy vân.

Để giải quyết nhược điểm của 2 phương pháo trên người ta thực hiện kết hợp thủy vân trong cả miền mới nhau. Ý tưởng là tách ảnh thủy vân ra thành 2 phần tương ứng với việc chèn trong miền không gian và tần số dựa trên sự ưu tiên của người dùng ở mức độ quan trọng dữ liệu.

Cách tách ảnh thủy vân thành 2 thành phần để chèn vào miền ko gian và miền tần số phụ thuộc vào yêu cầu của nguwoif dùng và phục thược vào ứng dụng. Về mặt nguyên tắc , thông tin quan trọng nhất xuất hiện ở phần trun tâm của ảnh. Do đó 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 chúng ta có thể cắt dữ liệu bí mật nhất để chèn vào miền tần số.

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

* Thuật toán:

Sơ đồ luồng:

Ảnh thủy vân trong miền không gian

Ảnh gốc

DCT

W1

Ảnh thủy vân kết hợp trong miền không gian và tần số

Thủy vân

DCT

W2

* Thuật toán:
* Tách thủy vân thành 2 phần:

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

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

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

M= M1 + M2

* Chèn W1 vào miền không gian của H để thu được :

HsHs= {hs(i,j) = h(i,j) W1 = {w1(i,j), 0≤i, j<N}, trong đó: h(i,j) và hs(i,j) thuộc { 0,1,2,..,2L-1},L là số bít đã dùng.

* Biến đổi Hs thành HDCT theo biến đổi DCT
* Chèn W2 vào các hằng số của HDCT thành HF:

HF= {hF(i,j) =hDCT(i,j) W2(i,j), 0≤ i, j< N}, trong đó: hF(i,j) thuộc { 0,1,2,..,2L-1}

* Biến đổi ảnh có nhúng thủy vân ở dạng DCT về dạng bình thường bằng phép biến đổi DCT ngược

# ***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:***

Sơ đồ thuật toán chèn thủy vân



Chèn vào LSB của

Khối ảnh có nhúng thủy vân

Đặt vào LSB =0

Khối ảnh đầu vào

Thuật toán chèn thủy vân:

1. Chia ảnh gốc X thành các ảnh con
2. Chia thủy vân W thành các thủy vân con
3. Vói mỗi ảnh con đặt LSB thành bit 0 để nhân
4. Vói mỗi dùng hàm băm(VD MD5 or SHA) để nhận được mã băm
5. là kq nhận được khi thực hiện XOR
6. bằng thuật toán RSA với khóa riêng để nhận được
7. vào LSB của để thu được ảnh con có thủy vân

*Sơ đồ trích xuất thủy vân:*

*Qr*

Đặt vào LSB =0

Khối ảnh đầu vào

Z

Trích xuất LSB

Ur Er

Thủy vân trích xuất được

Thuật toán trích xuất thủy vân:

1. Chia ảnh Z nhận được thành các
2. Đặt LSB của thành bit 0 kết quả thu đc .
3. Trích xuất LSB của nhận được
4. Giai mã bằng cách dùng RSA với khóa công khai K để thu được .
5. Với mỗi 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 cửa wrong có ddiemr 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.