TIỂU LUẬN

GIẤU TIN TRONG DỮ LIỆU ĐA PHƯƠNG TIỆN (STEGANOGRAPHY)

GVHD: NGUYỄN LINH GIANG

Nhóm sinh viên: Trần Thị Thúy 20173394

Dương Hồng Tuấn 20173439

Nguyễn Thị Duyên 20173076

Mục lục

Contents

Danh sách các từ viết tắt, thuật ngữ

Steganography

Crytography

Cover file

Stego file

Secret data

Danh mục các bảng, hình vẽ

Phần mở đầu

1. Lí do chọn đề tài

Xã hội ngày càng phát triển, cách mạng 4.0, thế giới số, thế giới phẳng,.. là những khái niệm mà ngày nay là rất quen thuộc với hầu hết mọi người. Càng ngày, nhu cầu về trao đổi thông tin càng lớn, dữ liệu con người tạo ra cũng ngày càng lớn, kéo theo đó là các vấn đề về bảo mật dữ liệu, bảo mật thông tin, bảo vệ bản quyền, ngăn chặn việc đánh cắp và sao chép tài liệu bất hợp pháp. Giấu tin với các kĩ thuật phù hợp có thể giải quyết được các vấn đề đặt ra. Với sự quan tâm về bảo mật thông tin và các lợi ích mà giấu tin đem lại, nhóm chúng em quyết định chọn đề tài giấu tin trong dữ liệu đa phương tiện.

Steganography đã trở nên ngày càng phổ biến trong những năm qua, do sự bùng nổ của internet và sử dụng đa phương tiện nói chung. Hầu hết sự chú ý đã được thu hút vì sử dụng kỹ thuật độc hại. Nó đã được sử dụng cho khủng bố, lừa đảo, gián điệp, vv...

Nó đã trở thành mối đe dọa không chỉ đối với các cá nhân và doanh nghiệp, mà còn đối với các cơ quan chính phủ và an ninh nội địa, không chỉ ở Hoa Kỳ, mà trên toàn thế giới. Đây là lý do tại sao bây giờ có một mối quan tâm ngày càng tăng trong phân tích Steganalysis, đó là phát hiện dữ liệu nhúng. Vấn đề là, có rất nhiều phương pháp để nhúng thông tin, thật khó để phát triển các chương trình để phân biệt giữa các loại khác nhau.

Có hơn 100 chương trình steganography miễn phí, chẳng hạn như Outguess, có sẵn trên internet, và được báo cáo rằng đã có hơn 1 triệu lượt tải xuống phần mềm này, cho thấy mức độ phổ biến của steganography đang trở nên như thế nào. Nó không phải luôn luôn được sử dụng theo cách xấu, một số người chỉ muốn giữ bí mật thông tin cá nhân của họ hoặc sử dụng nó như một cách khác để mã hóa thông tin quan trọng, nhưng thực tế là nó có thể được sử dụng theo cách hình sự, và đó là những gì mối quan tâm là về.

2. Tổng quan về đề tài

Giấu tin không phải là một khái niệm xa lạ, nó xuất hiện từ khá lâu, lịch sử giấu tin có thể nói là bắt đầu từ thời cổ đại, khi các chủ nhân dùng để cạo đầu nô lệ và sau đó viết tin nhắn trên đầu hoặc bất kỳ bộ phận cơ thể nào khác và sau đó gửi nô lệ của mình cho những người có liên quan.

3. Phạm vi nghiên cứu

4. Mục đích nghiên cứu

Tìm hiểu các khái niệm và các kĩ thuật cơ bản về giấu tin trong dữ liệu đa phương tiện.

5. Kết cấu

Nội dung

Chương 1: Các khái niệm cơ bản liên quan đến giấu tin trong dữ liệu đa phương tiện (Steganography)

1.1. Dữ liệu đa phương tiện là gì?

Phương tiện là đề cập tới các kiểu thông tin hay các kiểu thể hiện thông tin như dữ liệu số, văn bản, hình ảnh, âm thanh, video.

Dữ liệu đa phương tiện bao gồm một hoặc nhiều kiểu dữ liệu phương tiện truyền thông chính như văn bản, hình ảnh, các đối tượng đồ họa (bao gồm bản vẽ, phác thảo và hình minh họa) các chuỗi hình ảnh động, âm thanh và video.

Dữ liệu đa phương tiện xuất hiên trong mọi mặt đời sống xã hội như truyền thông, giải trí, thương mại, giáo dục,…và thường xuyên phải đối mặt với vấn đề bản quyền-quyền sở hữu trí tuệ đối với sản phẩm.

Đặc điểm của dữ liệu đa phương tiện:

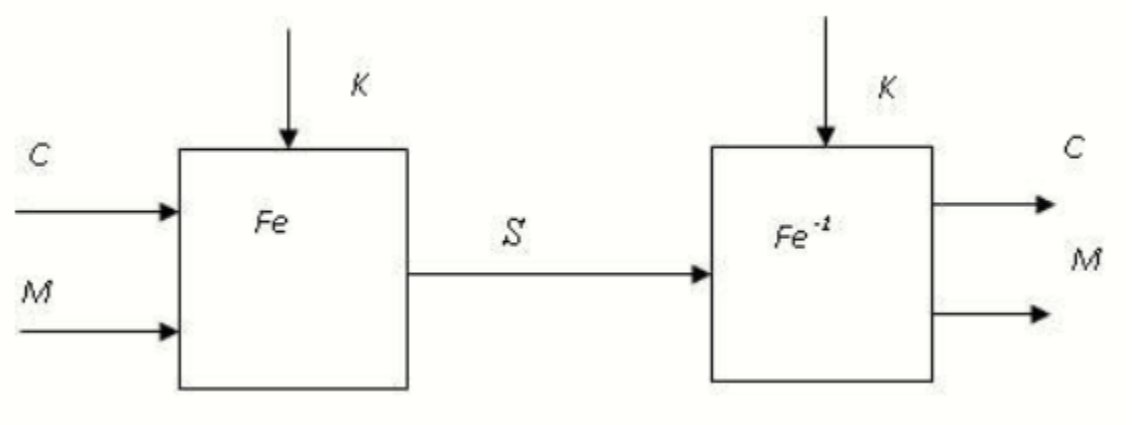
- Dung lượng lớn
- Đa dạng và phức tạp, phi cấu trúc

1.2. Steganography là gì?

Steganography là việc viết và chuyển tải các thông điệp một cách bí mật, sao cho ngoại trừ người gửi và người nhận, không ai biết đến sự tồn tại của thông điệp, là một dạng của bảo mật bằng cách che giấu. Steganography che giấu thông tin bằng cách ẩn thông tin vào 1 tệp dữ liệu khác (có thể là âm thanh, hình ảnh, text,..) gọi là tệp mang, sau đó gửi đi như một cách gửi tin thông thường, làm cho ngoại trừ người gửi và người nhận không ai có thể biết được có thông tin ẩn giấu, hoặc nếu biết có thông tin ẩn cũng không thể lấy được nội dung, chỉ có thể phá hủy tệp mang.

Các thành phần trong kỹ thuật giấu tin:

- Phương tiện chứa tin (cover media) (C) chứa thông tin ẩn
- Thông tin giấu (secret data) (M) có thể là văn bản thuần túy, văn bản mật mã hoặc bất kỳ loại dữ liệu nào.
- Hàm stego (Fe) và hàm nghịch đảo của nó (Fe^{-1})
- Khóa stego (K) hoặc mật khẩu có thể được sử dụng để giấu tin và lấy tin[2].



Hình 1 Sơ đồ giấu tin[2]

1.3. Mục đích của giấu tin

Mục tiêu của Steganography là che giấu các thông báo cần giữ bí mật trong các dữ liệu "vô hại" khác để đối phương không thể phát hiện được sự hiện diện của thông báo.

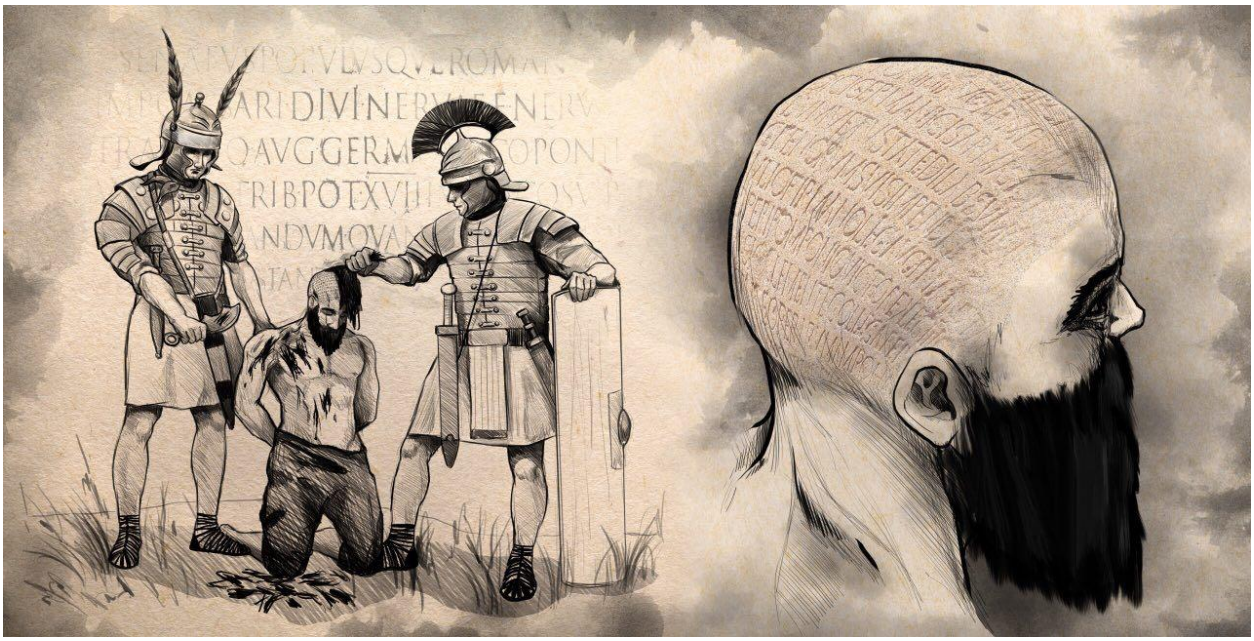
1.4. Yêu cầu của giấu tin

Có nhiều giao thức hay kỹ thuật nhúng tin khác nhau để ta có thể giấu dữ liệu, nhưng các giao thức, kỹ thuật này phải thỏa mãn một số yêu cầu:

- Tính toàn vẹn của dữ liệu giấu sau khi nó được nhúng vào đối tượng giấu tin phải chính xác.
- Đối tượng giấu tin phải được duy trì không đổi hoặc gần như không đổi với mắt thường.
- Trong thủy phân số, sự thay đổi của đối tượng giấu tin phải không ảnh hưởng đến chữ ký ảnh.
- Luôn luôn giả sử rằng kẻ tấn công biết rằng có dữ liệu được giấu trong đối tượng[1].

1.5. Lịch sử giấu tin

Khái niệm steganography được giới thiệu lần đầu tiên vào năm 1499, nhưng bản thân ý tưởng đã tồn tại từ thời cổ đại. Có những câu chuyện về một phương pháp đang được sử dụng trong Đế chế La Mã, theo đó một nô lệ được chọn để truyền tải một thông điệp bí mật đã cạo sạch tóc và một thông điệp được xăm trên da. Khi tóc của sứ giả mọc trở lại, anh ta được phái đi làm nhiệm vụ. Người nhận lại cạo tóc của người đưa tin và đọc tin nhắn.



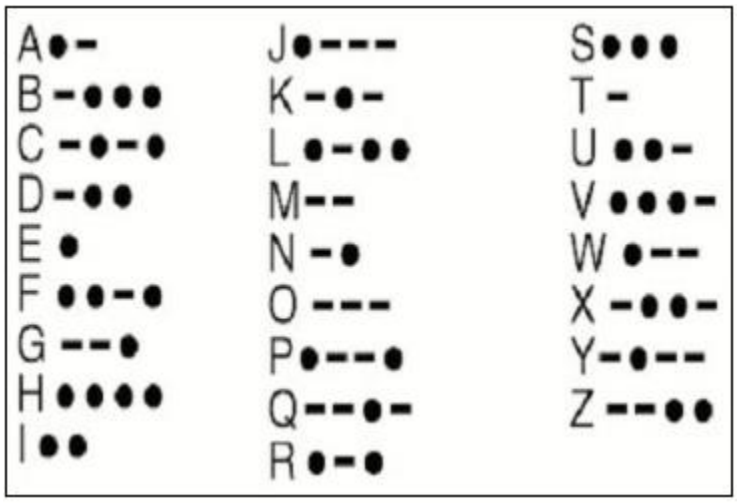
Hình 2 giấu tin thời cổ đại

Trong thế kỉ 20, mực vô hình trở thành một kĩ thuật được sử dụng rộng rãi. Trong chiến tranh thế giới thứ 2, con người sử dụng sữa, nước ép trái cây, giấm, nước tiểu để viết các tin nhắn bí mật. khi được làm nóng, các chất lỏng này trở nên sẫm màu, và tin nhắn có thể được đọc.

Hình 3: minh họa mực vô hình[7]

Một cách giấu tin khác là che giấu thông tin trong 1 quả trứng luộc bằng cách sử dụng một loại mực đặc biệt làm bằng 1 ounce phèn và nửa ounce giấm. dung dịch xuyên qua lớp vỏ trứng, nhuộm màu lên bề mặt của phần lòng trắng và không để lại giấu vết gì, tin nhắn có thể được đọc bằng cách loại bỏ lớp vỏ trứng.

Ngoài ra, còn có kĩ thuật mật mã null, microdots được sử dụng trong các cuộc chiến tranh thế giới, hoặc các tù nhân truyền đi thông điệp bằng cách nháy máy tạo ra mà Morse,…



Hình 4: mã Morse[7]

1.6. Phân biệt steganography và cryptography

Steganography thường bị nhầm lẫn với Cryptography bởi vì cả hai kỹ thuật này có ý định giữ dữ liệu một cách riêng tư, không để cho người không liên quan biết. Tuy nhiên, cả hai đạt được các mục tiêu rất khác nhau:

- Với Cryptography, bất kỳ kẻ nghe trộm nào cũng sẽ biết rằng thông tin trao đổi đã được mã hóa và không thể đọc được nếu không biết khóa giải mã.
- Steganography ngụy trang dữ liệu và truyền dữ liệu bằng phương tiện vận chuyển dường như vô hại để ngăn chặn kẻ rình mò biết rằng cuộc trao đổi bí mật đang diễn ra.

Cơ sở	Steganography	Cryptography
Mục tiêu	Che giấu sự tồn tại của các thông điệp, bằng cách ẩn nó vào một cái khác mà không gây chú ý.	Che giấu nội dung của thông điệp bằng cách đưa nó về dạng không thể hiểu được
Chiến thuật che giấu	Thông điệp được nhúng vào là vô hình đối với một người quan sát không biết.	Tin nhắn được mã hóa là không thể lấy được bởi bất kì ai mà không có khóa giải mã.
Nguyên tắc bảo mật	Bảo mật và xác thực	Bảo toàn, toàn vẹn dữ liệu, xác thực và chống phủ nhận
Kỹ thuật thực hiện	Miền không gian, miền biến dổi, biến dạng,..	Mã khóa khóa đổi xứng, bất đối xứng, chuyển vị, thay thế, mật mã dòng, mật mã khối,

Các kiểu tấn công	Steganalysis	Kỹ thuật đảo ngược, phân tích mật mã

Bảng 1: So sánh Steganography và Criptography

Secret Communication Techniques	Confidentiality	Integrity	Un removability
Encryption	Yes	no	Yes
Digital Signatures	No	Yes	No
Steganography	Yes/No	Yes/No	Yes

Bảng 2: So sánh cấc kỹ thuật truyền thông bí mật [1]

1.7. Phân loại giấu tin

Dựa vào loại tệp mang thông tin, chia thành:

- Steganography hình ảnh
- Steganography âm thanh và video
- Steganography văn bản
- Steganography IP datagram

Chương 2: Giấu tin trong ảnh

1. Khái niệm*Giấu tin trong ảnh* là việc thực hiện giấu thông tin với môi trường chứa là các file ảnh. Hiện nay, giấu tin trong ảnh chiếm tỉ lệ lớn trong các ứng dụng giấu tin trong dữ liệu đa phương tiện bởi vì lượng thông tin được trao đổi bằng hình ảnh là rất lớn. Giấu tin trong ảnh có nhiều ứng dụng trong thực tế, ví dụ như trong việc xác định bản quyền sở hữu, chống xuyên tạc thông tin hay truyền dữ liệu một cách an toàn,…

Các khái niệm thường được dùng trong giấu tin trong ảnh:

- *Ảnh môi trường:* Là ảnh gốc được dùng để nhúng thông tin.
- *Thông tin nhúng:* Là các thông tin mật cần gửi.
- *Ảnh đã nhúng:* Là ảnh gốc sau khi đã được nhúng thông tin mật.
- *Khóa mật:* Là khóa tham gia vào quá trình nhúng, được trao đổi giữa người gửi và người nhận.

Các yêu cầu trong giấu tin trong ảnh:

- *Tính bền vững:* Thể hiện khả năng ít bị thay đổi (về nội dung, hình dạng) trước những tấn công từ bên ngoài. Hiện nay, chưa có kỹ thuật giấu tin nào đảm bảo được yêu cầu này một cách tuyệt đối.

- *Khả năng không bị phát hiện:* Thể hiện ở việc khó xác định được đối tượng có chứa thông tin mật hay không. Các kỹ thuật giấu tin hiện nay cố gắng đảm bảo yêu cầu này dựa vào hệ thống thị giác của con người.
- *Khả năng lưu trữ:* Thể hiện ở lượng thông tin được lưu trữ. Do còn phải đảm bảo "khả năng không bị phát hiện" nên với những thông tin mật lớn, ta thường chia nhỏ nó ra, nhúng nhiều lần và vào các đối tượng khác nhau.

Các hình ảnh được chia thành ba loại:

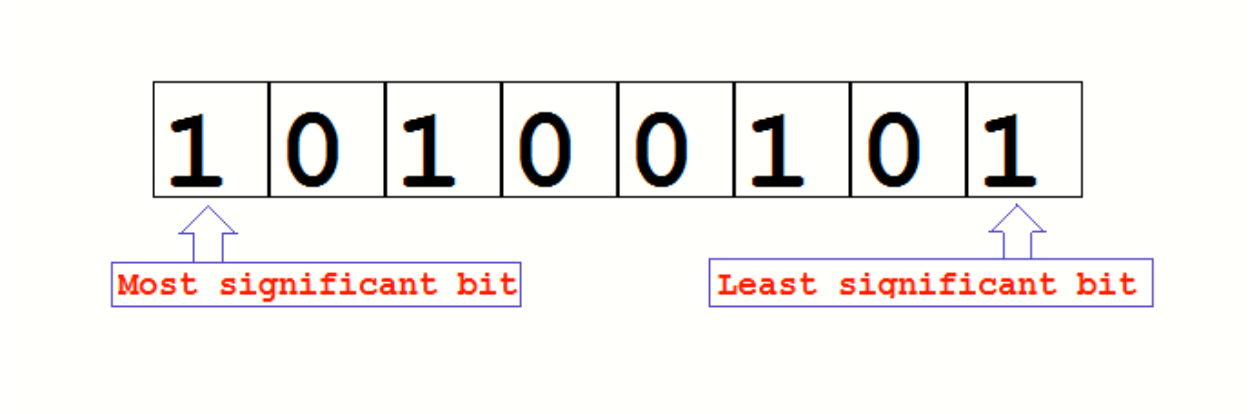
- Hình ảnh nhị phân (Đen-Trắng): có một giá trị bit trên mỗi pixel đại diện cho 0 cho màu đen và 1 cho pixel trắng
- Hình ảnh xám(Gray Scale) : có giá trị 8 bit cho mỗi pixel đại diện từ 00000000 cho màu đen và 11111111 cho pixel trắng
- Hình ảnh màu (RGB): có giá trị 24 bit trên mỗi pixel đại diện cho (00000000, 00000000 và 00000000) cho màu đen và (11111111, 111111 và 11111111) cho pixel trắng. Hình ảnh màu RGB là phù hợp nhất vì nó chứa nhiều thông tin giúp che giấu thông tin bí mật với một chút thay đổi về độ phân giải hình ảnh, không ảnh hưởng đến chất lượng hình ảnh và làm cho thông điệp an toàn hơn.

Có nhiều phương pháp khác nhau để giấu tin trong ảnh:

- Phương pháp tối thiểu bit (LSB)
- Chuyển đổi kỹ thuật miền
- Phương pháp thống kê
- Kỹ thuật biến dạng
- Thuật toán Hash-LSB và RSA

2. PhươngphápLeast significant bit (LSB) method

Least significant bit là các bit trong một byte mà khi ta xóa bit đó đi giá trị của byte đó gần như không đổi.



Hình 5: minh họa cho LSB

Phương pháp LSB giấu tin dựa vào khả năng nhận diện các sự thay đổi nhỏ về màu sắc, cường độ sáng của mắt người là rất kém. Về nguyên tắc, mắt thường không thể quan sát được hai mức màu kề nhau[9].

Với mỗi loại ảnh khác nhau, giấu tin bằng phương pháp LSB cũng khác nhau:

- Đối với ảnh màu 24-bit: mỗi ảnh là sự thể hiện của 3 kênh màu riêng biệt red, green, blue. Mỗi pixel ảnh là sự thể hiện đồng thời của 3 màu này, với giá trị tại mỗi pixel của mỗi mày nằm trong đoạn [0, 255]. Chính vì vậy, giấu tin bằng phương pháp LSB trên ảnh màu, mỗi pixel ta có thể giấu được 3 bit thông điệp.
- Đối với ảnh đa cấp xám (8-bit), mỗi pixel chứa một giá trị nằm trong khoảng [0,255] và giấu được 1 bit thông điệp.
- Ảnh nhị phân, mỗi pixel chứa giá trị 0 hoặc 1. Giấu tin bằng LSB trên ảnh nhị phân rất dễ bị phát hiện bởi sự xuất hiện của các chấm đen trên nền trắng hặng chấm trắng trên nền đen là rất dễ bị chú ý, đối với ảnh loại này, chỉ nên giấu tin vào các pixel ở khu vực viền của các đối tượng trong ảnh, viền giao nhau giữa màu đen và trắng.

  Thực hiện giấu tin bằng LSB:

  1. Chuyển thông điệp về dạng nhị phân
  2. Đọc từng pixel của ảnh, lần lượt thay thế các bit cuối cùng của mỗi pixel tương ứng với một bit nhị phân của thông điệp.

  Lấy tin:

  1. Đọc từng pixel của ảnh chứa tin giấu
  2. Tại mỗi pixel, lấy ra bit cuối cùng, ghi và một file mới
  3. Từ file mới thu được, chuyển dữ liệu về dạng kí tự để thu được thông điệp.

  Ta có thể tăng khả năng giấu tin bằng cách tăng thêm số lượng bit bị thay thế lên 2 hoặc 3 bit.

Một nhược điểm của phương pháp này là thông điệp dễ bị phá hủy với các phép biến đổi đơn giản, phép nén dữ liệu ảnh, các phép biến đổi hình học như di chuyển các điểm ảnh, đổi chỗ các điểm ảnh…hơn nữa quá trình giải tin là rất dễ, chính vì vậy, cần kết hợp thêm một số phương pháp bảo mật khác như mã hóa thông điệp trước khi nhúng vào ảnh…

2.2 Giải thuật Hash-LSB and RSA

A. Ảnh chứa tin và thông điệp mật:

Trong hệ thống được đề xuất của Ravi K Sheth và Rashmi M. Tank, trước hết họ chọn một hình ảnh màu thực có kích thước 512 x 512 cho nó làm ảnh bìa và một thông điệp bí mật sẽ được nhúng vào ảnh bìa.

B. Quá trình Hash-LSB

Kỹ thuật Bit thấp dựa trên bảng băm (H-LSB) để ghi bản sao trong đó vị trí của LSB để ẩn dữ liệu bí mật được xác định bằng hàm băm. Hàm băm tìm vị trí của bit thấp nhất của từng pixel RGB và sau đó các bit thông điệp được nhúng độc lập vào các pixel RGB RGB này.

Sau đó, hàm băm trả về giá trị băm theo các bit thấp nhất có trong các giá trị pixel RGB. Ảnh chứa tin sẽ được chia nhỏ hoặc phân mảnh thành định dạng RGB. Sau đó, kỹ thuật Hash LSB sẽ sử dụng các giá trị được cung cấp bởi hàm băm để nhúng hoặc che giấu dữ liệu.

Trong kỹ thuật này, thông điệp bí mật được chuyển đổi thành dạng nhị phân dưới dạng bit nhị phân; mỗi 8 bit tại một thời điểm được nhúng vào các bit có giá trị pixel RGB tối thiểu của ảnh bìa theo thứ tự lần lượt là 3, 3 và 2. Theo phương pháp này, 3 bit được nhúng vào LSB pixel màu đỏ, 3 bit được nhúng vào LSB pixel màu xanh lá cây và 2 bit được nhúng vào LSB pixel màu xanh . 8 bit này được chèn theo thứ tự này vì ảnh hưởng màu sắc của màu xanh biển đối với mắt người nhiều hơn màu đỏ và màu xanh lá cây. Do đó, mẫu phân phối chọn 2 bit được ẩn trong pixel màu xanh biển. Do đó, chất lượng của hình ảnh sẽ không bị hy sinh.

Công thức sau đây được sử dụng để phát hiện các vị trí để ẩn dữ liệu trong LSB của từng pixel RGB của ảnh chứa tin:

k = p% n, ..,. (1)

Trong đó :

k là vị trí bit LSB trong pixel;

p đại diện cho vị trí của từng pixel ảnh ẩn

n là số bit của LSB mà là 4 cho trường hợp hiện tại.

Sau khi nhúng dữ liệu vào ảnh , một ảnh stego sẽ được tạo ra. Người nhận hình ảnh này phải sử dụng lại hàm băm để trích xuất các vị trí lưu trữ dữ liệu. Các thông tin được trích xuất sẽ có trong văn bản mật . Sau khi giải mã nó, việc kết hợp các bit thành thông tin sẽ tạo ra thông điệp bí mật theo yêu cầu của người nhận.

C. Mã hóa RSA và Mã hóa Hash-LSB

Cách tiếp cận này của giấu tin trong hình ảnh đang sử dụng kỹ thuật mã hóa RSA để mã hóa dữ liệu bí mật. Sau khi mã hóa, phương thức Hash-LSB được áp dụng trên bản mã.

Thuật toán truy xuất giải mã Hash-LSB và giải mã RSA:

Bước 1: Nhận hình ảnh stego.

Bước 2: Tìm 4 bit LSB của mỗi pixel RGB từ hình ảnh stego.

Bước 3: Áp dụng hàm băm để có được vị trí của LSB dữ liệu với dữ liệu ẩn.

Bước 4: Lấy các bit bằng các vị trí này theo thứ tự lần lượt là 3, 3 và 2.

Bước 5: Áp dụng thuật toán RSA để giải mã dữ liệu đã truy xuất.

Bước 6: Cuối cùng đọc thông điệp bí mật.

Mục tiêu của công việc đã được thực hiện một kỹ thuật chụp ảnh bản đồ bằng phương pháp Hash-LSB (Least Significant Bit) với thuật toán RSA để cải thiện tính bảo mật của kỹ thuật che dấu dữ liệu.

Chương 3: Giấu tin trong dữ liệu audio

Giấu tin trong dữ liệu audio dựa vào ngưỡng nghe của người và hiện tượng che khuất âm thanh[11].

3.1. Ngưỡng nghe và hiện tượng che khuất âm thanh

Phạm vi nghe của con người là khoảng (20Hz, 20kHz), nhưng nghe rõ nhất với âm thanh trong khoảng (1kHz, 4kHz). Ngưỡng nghe có sự khác nhau đối với từng người, giới tính, độ tuổi.

Mặc dù con người có thể nghe được ở dải tần rộng nhưng những gì con người nghe được phụ thuộc vào môi trường nơi nghe. Trong môi trường nhiễu mạnh, các âm thanh nhỏ sẽ bị che khuất, khiến cho con người không thể nghe được.

Hiện tượng che khuất tín hiệu âm thanh (auditory masking) xảy ra khi một âm thanh này ảnh hưởng đến sự cảm nhận một âm thanh khác. Âm thanh bị che gọi là maskee, âm thanh che là masker. Khoảng cường độ khác nhau giữa maskee và masker gọi là mức độ che.

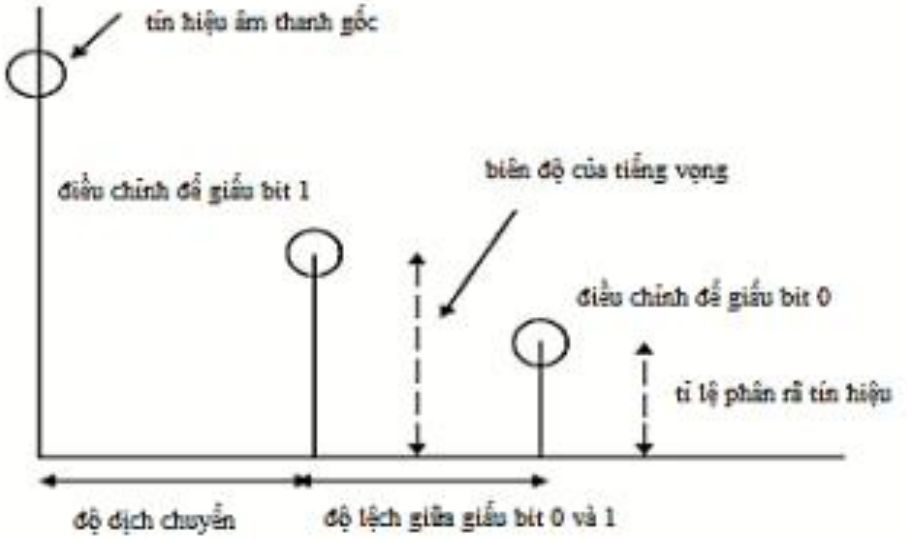
Để xử lý và lưu trữ âm thanh bằng máy tính, các tín hiệu âm thanh phải được chuyển từ dạng tương tự sang dạng số. Một mẫu dữ liệu âm thanh có thể được biểu diễn bằng 8 bit, 16 bit, 24 bit.

3.2. Mã hóa LSB (least significant bit)

Mã hóa LSB là phương pháp nhúng dữ liệu bằng cách thay thế các bit có trọng số thấp của mẫu dữ liệu audio bằng bit thông tin giấu.
Phương pháp này dễ cài đặt, thời gian thực hiện nhanh, và ta có thể thêm dữ liệu giấu bằng cách dùng 2 bit LSB, tuy nhiên, có thể làm tăng nhiễu trên đối tượng khiến đối phương dễ phát hiện và thực hiện tấn công.
Để tăng độ an toàn , ta sử dụng một bộ sinh số ngẫu nhiên để sinh ra các vị trí các mẫu được chọn[10].

3.3. Kỹ thuật giấu dựa vào tiếng vang (echo)

Dựa trên đặc trưng của hệ thống thính giác của con người không phân biệt được 2 âm thanh nếu chúng có gần như xảy ra đồng thời (độ lệch trong khoảng (1, 40ms).
Kỹ thuật này giấu tin bằng cách thêm các bit thông tin vào tiếng vang trong dữ liệu audio gốc bằng cách thay đổi 3 thông số của tiếng vang: biên độ ban đầu, tỉ lệ phân rã và độ trễ.
Khi thời gian giữa tín hiệu gốc và tiếng vang giảm xuống, hai tín hiệu có thể trộn lẫn và người nghe khó có thể phân biệt giữa hai tín hiệu. Số lượng tin giấu có liên quan ñến thời gian trễ của tiếng
vang và biên độ của nó.

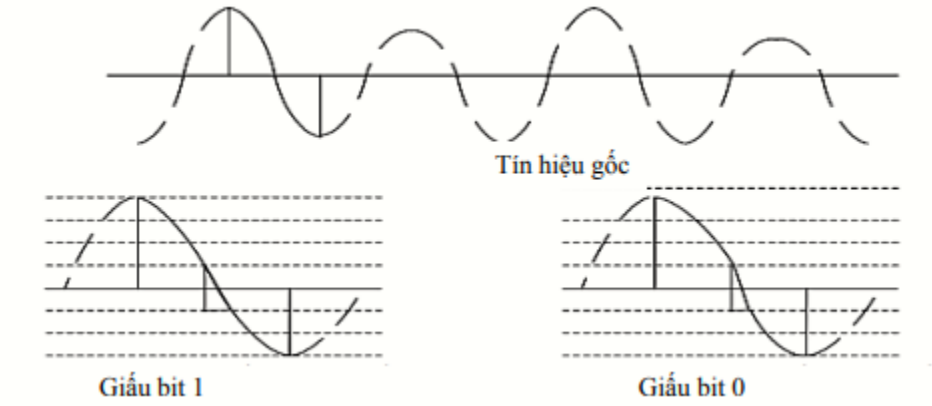


Hình 6: Các thành phần trong tiếng vang của tín hiệu [11]

Bằng cách chọn thời gian trễ khác nhau giữa tín giệu gốc và tiếng vang để thể hiện tương ứng bit 0, 1. Hai độ trễ có thể được chọn cố định hoặc phụ thuộc vào khóa[11].

3.4. Phương pháp điều chế tỉ lệ thời gian

Ý tưởng cơ bản của phương pháp này là thay đổi tỉ lệ thời gian giữa hai cực của đoạn xét, ta thay đổi độ dốc của tín hiệu tùy thuộc vào bit muốn nhúng. Dôc thoải để giấu bit 1, dốc đứng để giấu bit 0.



Hình 7: điều chỉnh độ dốc để giấu thông tin[11]

Chương 4: Giấu tin trong văn bản text

Giấu tin trong văn bản là kỹ thuật giấu tin khó nhất trong các loại giấu tin, bởi vì file văn bản có lượng thông tin dư thừa là rất nhỏ để giấu được thông điệp.

Một số phương pháp giấu tin trong văn bản:

1. Syntactic method:
   Moerland đưa ra một phương pháp giấu tin trong văn bản bằng cách sử dụng các dấu ngắt câu như dấu chấm (.), dấu phảy (,), dấy chấm phẩy (;),… trong văn bản để ẩn các bit 0, 1. Phương pháp này sẽ rất là khó để cho những kẻ xâm nhập nhận ra là có thông điệp được nhúng trong đó, vì việc sử dụng các dấu ngắt câu là rất bình thường, phổ biến trong một văn bản. Tuy nhiên cũng cần phải để ý vì các dấu câu phải đặt đúng vị trí của nó nếu không người đọc sẽ nghi ngờ[4].
2. Line shifting method
   Phương pháp này nhúng dữ liệu cần giấu vào một đoạn text bằng cách thay đổi khoảng giãn cách giữa các dòng. Dữ liệu được truyền vào dưới dạng chuỗi nhị phân, với cách dòng có khoảng giãn cách là l biểu thị cho bit 0, các dòng có khoảng giãn dòng là l+Δ biểu thị cho bit 1[5].
   Tuy nhiên phương pháp này chỉ phù hợp khi mà các chương trình nhận dạng chữ cái (OCR) không được sử dụng. Khi sử dụng các OCR, thông tin dược giấu sẽ bị mất.
3. Word shifting
   Phương pháp này gần giống như line shifting, nhưng khác ở chỗ nó ẩn các bit 0, 1 bằng cách giãn cách khoảng cách giữa các từ với nhau. Phương pháp này cuingx khá là dễ để thực hiển, bởi vì việc giãn cách các từ cho phù hợp với dòng là khá bình thường. tuy nhiên, nếu ai đó biết các thuật toán về word shifing distance, có thể dễ dàng lấy được thông tin ẩn. hoặc thông tin ẩn sẽ bị mất nếu như sử dụng các chương trình nhận diện chữ cái (OCR) hay ai đó gõ lại nội dung văn bản.
4. Giấu dữ liệu trong đoạn văn [4]
   Phương pháp này sử dụng tập cover file là một đoạn văn bản tiếng Anh có thể được rút trích từ bất cứ nguồn nào, với bất kì ý nghĩa nào.
   Phương pháp này giấu tin như sau:
   1. Chọn 1 tệp để giấu thông tin vào đó (tệp cover)
   2. Chuyển đổi nội dung thông điệp thành chuỗi bit 0, 1 gọi là bin.
   3. Đọc từng bit trong bin
   4. Đọc từng từ trong tệp được chọn để mang thông điệp, và viết nó vào trong stego file.
   5. Nếu chữ cái bắt đầu và chữ cái kết thúc của từ là giống nhau thì đọc từ tiếp theo của tệp cover và viết nó vào stego file.
   6. Đặt s = chữ cái bất đầu của từ, e = chữ cái kết thúc của từ

7. Nếu cần giấu bit 0 thì viết s vào khóa stego
8. Nếu cần giấu bit 1 thì viết e vào khóa
9. Lặp lại cac bước từ 3 đến 8 cho đến khi đọc hết bin
10. Gửi stego file và khóa tương ứng đến người nhận.

Thuật toán tìm thông điệp:

1. Đọc từ chữ cái (c) từ khóa stego nhận được
2. Đọc từ từ từ stego file nhận được
3. Nếu chữ cái bắt đầu và kết thúc của từ là giống nhau thì bỏ qua từ đó vầ đọc từ tiếp theo
4. Đưa ra các chữ cái bắt đầu (s) và kết thúc (e) của từ
5. Nếu c=s thì bit giấu là 0, nếu c=e thì bit giấu là 1
6. Viết bit vừa tìm được ra một file mới
7. Lặp lại các bước cho đến khi đọc hết khóa
8. Chuyển đổi file chứa các bit tìm được thành các kí tự tương ứng để thu được thông điệp.

Chương 5: Giấu tin trong video

1.5.Video và cấu trúc định dạng một số tệp Video

1.5.1. Khung và cấu trúc khung trong video.

Video bao gồm một loạt các ảnh bitmap trực giao hiển thị trong liên kết nhanh với tốc độ không đổi. Trong cấu trúc của video những ảnh này được gọi là khung hình. Chúng ta đo tốc độ khung hình được hiển thị trong mỗi giây (FPS).

Vì mỗi khung hình là một ảnh kỹ thuật số trực giao bitmap bao gồm một raster các điểm ảnh (pixel). Nếu nó có chiều rộng W pixel và chiều cao H pixel ta nói rằng kích thước khung hình là W x H pixels.

Pixels chỉ có một thuộc tính màu sắc của chúng. Màu sắc của một điểm ảnh được biểu diễn bởi một giá trị cố định các bit. Các bit hơn các biến thể tinh tế của màu sắc là có thể được sao chép. Đây được gọi là độ sâu màu (CD) của video.

Ví dụ video có thể có thời gian (T) 1 giờ (3600 giây), kích thước khung hình 640 x 480 (R x C) ở độ sâu màu 24 bit và tỷ lệ khung hình 25 fps. Video ví dụ này có các thuộc tính sau:

 Pixel mỗi khung hình = 640 * 480 = 307.200

 Bit trên mỗi khung hình = 307.200 * 24 = 7.372.800 = 7, 37 Mbits

 Tỷ lệ bit (BR) = 7.37 * 25 = 184, 25 Mbits / sec

 Kích thước video (VS) = 184 Mbits / sec * 3600 giây = 662.400 Mbits = 82.800 MB = 82, 8 GB

Các đặc tính quan trọng nhất là tốc độ bit và kích thước video. Các công thức liên quan giữa hai thuộc tính đó với tất cả các thuộc tính khác là:

BR = W * H * CD * FPS VS = BR * T = W * H * CD * FPS * T

(Đơn vị là: BR theo bit/s, W và H theo điểm ảnh, CD bằng bit, VS theo bit, T theo giây)

Trong khi một số công thức thứ cấp là:

pixels_per_khung hình = W * H

pixels_per_second = W * H * FPS

bits_per_khung hình = W * H * CD

1.5.2. Một số loại định dạng video phổ biến

1.5.2.1. Đinh dạng AVI

Định dạng AVI (Audio Video Interle) là một định dạng số đa phương tiện do Microsoft giới thiệu vào tháng khoảng 11/1992 như một chuẩn video dành cho Windows. Tệp AVI có thể chứa cả dữ liệu âm thanh và video trong một tệp, cho phép đồng bộ với phát lại audio – video. Đặc điểm của tệp AVI là dạng video không nén, chính vì vậy hình ảnh của video dạng này khá đẹp và sắc nét, đây là đặc tính ưu điểm và đồng thời cũng là nhược điểm của định dạng này, vì không hình ảnh và âm thanh của nó được nén nên dung lượng của một tệp AVI thường khá lớn (một tệp video avi khoảng 60 phút sẽ có dung lượng khoảng trên dưới 10Gb)

1.5.2.2. Định dạng FLV (Flash video):

Tệp FLV là một dạng file nén từ các file video khác để tải lên trang web với dung lượng nhỏ, tuy nhiên chất lượng của hình ảnh không bằng được file gốc (MP4, WAV,…). Tệp FLV được lựa chọn cho việc nhúng video trong web, đây là định dạng hay được sử dụng bởi ứng dụng trên web như: Youtube, Google Video, Yahoo! Video,…

1.5.2.3. H.264/MPEG – 4 Part 10 hay AVC (Advanced Video Coding)

Đây là một chuẩn mã hóa/giải mã video và định dạng tệp video đang được sử dụng rộng rãi nhất hiện này vì khả năng ghi, nén và chia sẽ video phân giải cao. Tệp này có dung lượng thấp nhưng mang lại chất lượng rất cao.

1.5.2.4. H.263

H.263 được sử dụng rộng rãi trên internet như tệp FLV, hay sử dụng trong hội nghị, truyền hình, điện thoại video, giám sát và theo dõi.

1.4.2.5. WMV WMV (Windows Media Video) là một định dạng video chính quy mà bạn hay gặp hàng ngày. Tệp Windows Media chứa video được mã hóa theo bộ code Windows Media Video và âm thanh được mã hóa theo codec Windows Media Audio codec.
1.5.2.5. MPEG-4 Part 14 hoặc MP4

Là định dạng thường được sử dụng để lưu trữ video và âm thanh, nhưng cũng có thể được sử dụng để lưu trữ dữ liệu khác như phụ đề và hình ảnh. MP4 cho phép truyền tải trên Internet.

1.5.2.6. DivX (Digital Video Express)

Là một định dạng nổi tiếng từ lâu trong nhóm MPEG-4. Chất lượng coi như bằng MPEG 2 nhưng kích thước chỉ nhỏ bằng một nửa.

1.5.2.7. XviD (viết ngược lại của DivX)

Là một dạng MPEG4. XviD kết hợp hài hòa giữa tốc độ, chất lượng, có khả năng tùy biến cao, là một ASP code được giới chuyên môn đánh giá cao nhất.

1.5.2.8. 3GP

Là phiên bản đơn giản của MP4, được thiết kế để nén và giảm dung lượng cũng như băng thông cần thiết. Định dạng này sử dụng cho các ứng dụng trên máy điện thoại đi động thông minh. Nó lưu trữ hình ảnh như là MPEG-4 hay H.263 và âm thanh là dạng AMR-NB hay AAC-LC. Một tệp 3GP thường chứa nhiều nội dung nhiều hơn nội dung truyền tải, vì nó còn chứa các thông tin chú thích của hình ảnh.

1.5.2.9. MKV

Trái ngược với nhiều định dạng video khác, tệp tin MKV không phải là một định dạng nén âm thanh hoặc video. Tệp MKV là một tệp thực sự chứa đa phương tiện, nó có thể kết hợp âm thanh, video và phụ đề vào một tập tin duy nhất ngay cả khi chúng sử dụng mã khác nhau. Bạn có thể có một tập MKV sử dụng video VP8 với âm thanh Vorbis, hoặc phổ biến hơn sử dụng H.264 cho video và một cái gì đó giống MP3 hay ACC cho âm thanh.

1.5.2.10. MOV

Là một định dạng được Apple phát triển. Đây là một định dạng đa phương tiện phổ biến, thường được dùng trên Internet do ưu điểm tiết kiệm dung lượng của nó.

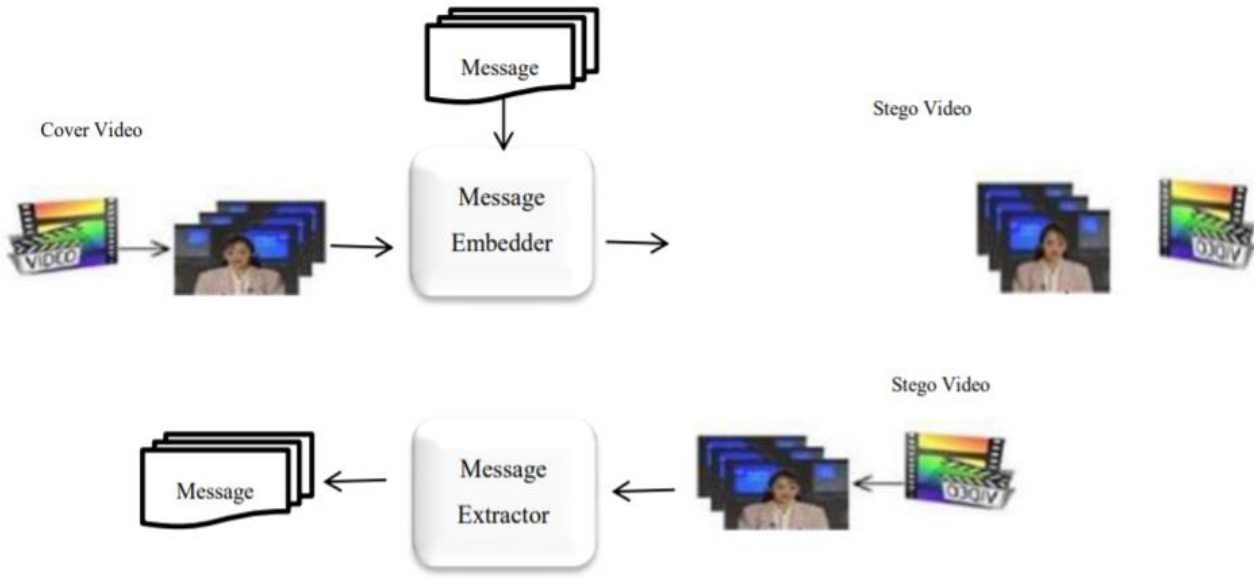
1.5.2.11. H.265

Hay còn gọi là HEVC (High Efficiency Video Coding – code video hiệu suất cao) là một định dạng video mang lại khả năng nén cao gần gấp đôi so với H.264/AVC hiện đang được dùng phổ biến, do đó giúp giảm băng thông cần thiết để truyền tải phim, đặc biệt là

trên các thiết bị di động. Nhờ đó, chúng không phải trả quá nhiều chi phí xem phim kết nối với 3G/4G mà vẫn thưởng thức được video chất lượng cao, thời gian tải nội dung cũng giảm đi.

1.6.Sơ đồ giấu tin và tách tin trong video

Sơ đồ giấu tin và tách tin trong video tổng quan được minh họa theo hình:



Hình 1.6. Quá trình giấu và tách thông tin trong video

Trong đó:

- Cover Video: là video ban đầu dùng để che giấu thông tin

- Message: là dữ liệu quan trọng cần giấu

- Message Embedder: bộ chương trình giấu tin

- Stego video: là video đã giấu tin

- Message Extractor: bộ chương trình tách thông tin đã giấu trong video Message đem giấu có thể là một đoạn văn bản, một ảnh logo, một đoạn mã ID định danh nào đó liên quan đến bản dữ liệu số che giấu nó hoặc có thể lại là một đoạn âm thanh số ngắn nào đó

1.7.Tăng tính an toàn cho thông tin đem giấu

Mặc dù giấu tin trong video là vô hình so với các phương pháp an toàn bảo mật khác. Tuy nhiên trong trường hợp nghi ngờ kẻ tấn công có thể sử dụng tìm mọi cách để tách thông tin mật ra khỏi video. Trong trường hợp này để tăng độ an toàn cho thông tin đem giấu có thể sử dụng phương pháp mã hóa cho thông tin mật trước khi giấu sử dụng các kỹ thuật mã hóa như RSA, Elgama, AES hoặc DES... hoặc có thể sử dụng phương pháp mã

hóa đơn giản đó là chuyển thông tin giấu sang chuỗi bit nhị phần, sau đó sự dụng phép toán XOR của chuỗi bit thông điệp với chuỗi khóa.

1.8. Đánh giá chất lượng âm thanh hoặc khung hình sau khi đã giấu tin

Để đánh giá chất lượng của tín hiệu âm thanh và khung hình của video đã giấu tin có thể sử dụng hai tham số: Sai số bình phương trung bình – MSE (Mean Square Error) và phương pháp hệ số tỷ lệ tín hiệu / tín hiệu nhiễu PSNR (Peak Signal to Noise Ratio).

MSE giữa tín hiệu gốc và tín hiệu đã giấu tin được tính như sau:

$$\text{MSE} = \frac{1}{N}\sum_{i=1}^{N}(x_i - y_i)^2$$

Ở đây:

xi biểu thị giá trị tín hiệu gốc

yi biểu thị giá trị tín hiệu đã bị biến đổi

N là độ dài của tín hiệu âm thanh.

PSNR, đơn vị: deciben (dB), thường được sử dụng trong xử lý tín hiệu số:

$$\text{PSNR} = 10*\log10\left(\frac{\max(x_i)^2}{MSE}\right)$$

2. Phương pháp giấu tin trong vide

Chi tiết về cấu trúc của tệp Video là sự kết hợp của các khung hình và âm thanh, do đó việc giấu tin trong video thực chất là sự kết hợp của giấu tin trong các khung hình (giống như giấu tin trong ảnh) và trong âm thanh. Sau đây là chi tiết một số phương pháp giấu tin trên khung hình và âm thanh của video.

2.1. Giấu thông tin trên LSB của khung hình video.

Một video bao gồm nhiều khung hình, ta có thể thực hiện giấu thông tin mật bằng cách chọn một số khung hình của video rồi giấu tin trên miền LSB của khung hình.

2.1.1. Miền bit trọng số thấp LSB (Least Significant Bit)

Bit trọng số thấp là bit ảnh hưởng ít nhất tới màu sắc hay chất lượng của mỗi điểm ảnh hoặc tín hiệu của dữ liệu âm thanh, vì vậy khi ta thay đổi giá trị của bit này thì màu sắc của điểm ảnh hay chất lượng âm thanh đó gần như không đổi.

Xác định LSB của mỗi điểm ảnh phụ thuộc vào định dạng của ảnh và số bit màu dành cho mỗi điểm của ảnh đó. Giả sử với ảnh 16 bit màu thì 15 bit dùng để biểu diễn màu RGB, bit còn lại không dùng đến có thể giấu tin, với ảnh 8 bit màu thì 7 bit đầu là bit quan trọng MSB (Most Significant Bit) bit còn lại là bit LSB. Giả sử hình 2.1 a) biểu diễn

nhị phân của bốn điểm ảnh khi đó ta có thể dễ dàng giấu 4 bit thông tin ”1100” được kết quả là hình 2.1. b). Khi quan sát kỹ chúng ta thấy việc thay đổi trên LSB này chỉ ảnh hưởng tới 50% các bit LSB, vì nếu coi miền bit LSB là đại lượng ngẫu nhiên thì khả năng trùng khớp theo thống kê là 50%.

a) 1010100 1 1110010 0 1101110 1 1111111 0

b) 1010100 1 1110010 1 1101110 0 1111111 0

Hình 2.1. a) biểu diễn nhị phân 4 điểm ảnh, b) kết quả thay đổi các LSB bằng chuỗi ”1100”

Với trường hợp tín hiệu âm thanh được lấy mẫu với tần số lấy mẫu là 44.1kHz thì tín hiệu có thể biểu diễn dưới dạng 16 bit khi đó chúng ta có thể giấu trên 1 đến 8 bit LSB của tín hiệu.

2.1.2. Phương pháp giấu tin trên LSB của khung hình video

Ý tưởng của phương pháp chính là giấu trên miền LSB của khung hình nào đó được chọn trong video. Nếu số lượng thông tin giấu lớn chúng ta có thể chọn giấu trên nhiều khung hình. Thuật toán giấu tin và tách tin có thể trình đơn giản sau đây:

Thuật toán giấu tin:

Đầu vào: Video gốc che giấu thông tin, thông điệp cần giấu

Đầu ra: Video đã giâu tin

Các bước thực hiện:

B1. Chọn ngẫu nhiên khung hình để giấu tin, khung hình này có thể biểu diễn lại dưới dạng ma trận điểm ảnh

B2. Biểu diễn thông điệp dưới dạng chuỗi nhị phân

B3. Chọn điểm ảnh P có thể theo thứ tự lần lượt hoặc giả ngẫu nhiên, B là bit thông tin cần giấu ta thực hiện các phép toán giấu tin sau: (Giả sử P là điểm ảnh 8 bit)

S=P and 255 or B

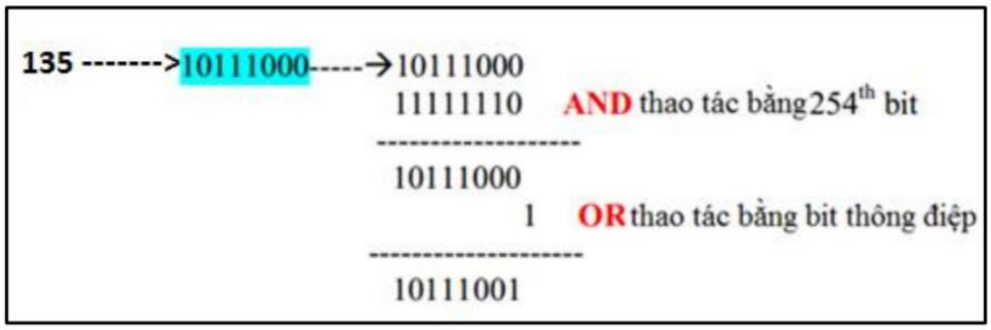
S: là điểm ảnh đã giấu tin

Hai tín hiệu ban đầu Thông điệp Hai tín hiệu ban đầu bị làm mù 8 bit LSB Hai tín hiệu đã giấu tin

(nếu là 24 bit ta sẽ thực hiện giấu lần lượt trên 3 kênh RGB)

B4. Lặp lại B3 cho đến khi giấu hết các bit thông điệp. Nếu thông điệp quá lớn so với khả năng tải trọng của một khung hình, sẽ thực hiện tiếp trên khung hình khác đến khi giấu hết thông tin.

Hình 2.3 là một minh họa giấu tin trên điểm ảnh có giá trị "135". Muốn tăng độ an toàn cho thông điệp có thể mã hóa thông điệp trước khi đem giấu.



Hình 2.3. Minh họa giấu tin LSB trên một điểm ảnh của khung hình

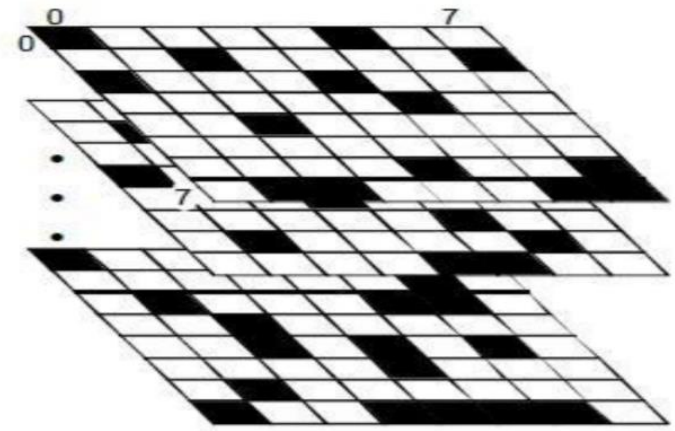
2.2.Giấu tin trên khung hình video bằng mặt phẳng phân đoạn nhiễu BPCS.

Kỹ thuật giấu tin trên miền bit LSB có ưu điểm là đơn giản và có thể giấu một lượng thông tin lớn tương đương với tỉ lệ kích thước của các khung hình, tuy nhiên giấu tin này còn gọi là giấu tin "dễ vỡ" vì chúng dễ dàng bị tấn công bằng phương pháp thống kê cặp điểm ảnh POV [2], hoặc các kỹ thuật hình học trong xử lý ảnh như: nén, làm mịn, co giãn ảnh, … Vì vậy trong phần này sẽ đưa ra một phương pháp giấu thứ hai giảm thiểu phần nào nhược điểm của phương pháp giấu trên LSB đó là kỹ thuật giấu tin trên khung hình sử dụng phân đoạn mặt phẳng bit nhiễu - BPCS (Bit Plane Complexity Segmentation steganography).

Ý tưởng chính của BPCS là giấu tin trên các vùng nhiễu thay vì giấu trên tất cả các vùng, nếu giấu trên các vùng đồng màu sẽ ảnh hưởng không nhỏ đến chất lượng ảnh, đặc biệt khi các khung hình của video được chiếu trên màn hình tivi lớn hay màn ảnh rộng việc gây ra nhiễu sắc màu cho các vùng này sẽ dễ bị ghi ngờ hơn.

Để hiểu khái niệm của mặt phẳng BPCS trước tiên chúng ta tìm hiểu khái niệm thế nào là một mặt phẳng bit của các điểm ảnh trong khung hình video. Số bit của mỗi điểm ảnh có thể là 8, 24 hoặc 32 bit. Giả sử một khung hình mà mỗi điểm ảnh được biểu diễn bởi 8 bit thì ta sẽ có 8 mặt phẳng bit tương ứng như minh họa trong hình 2.4, trong đó giả sử một điểm ảnh biểu diễn dưới dạng nhị phân là 01001110, trong mặt phẳng bit các màu đen ứng với giá trị 0 và màu trắng ứng với giá trị 1, do đó trong mặt phẳng bit thứ nhất tại vị tri (0,0) có một màu đen (biểu diễn giá trị 0), trong mặt phẳng bit thứ 2 tại vị trí (0,0) có

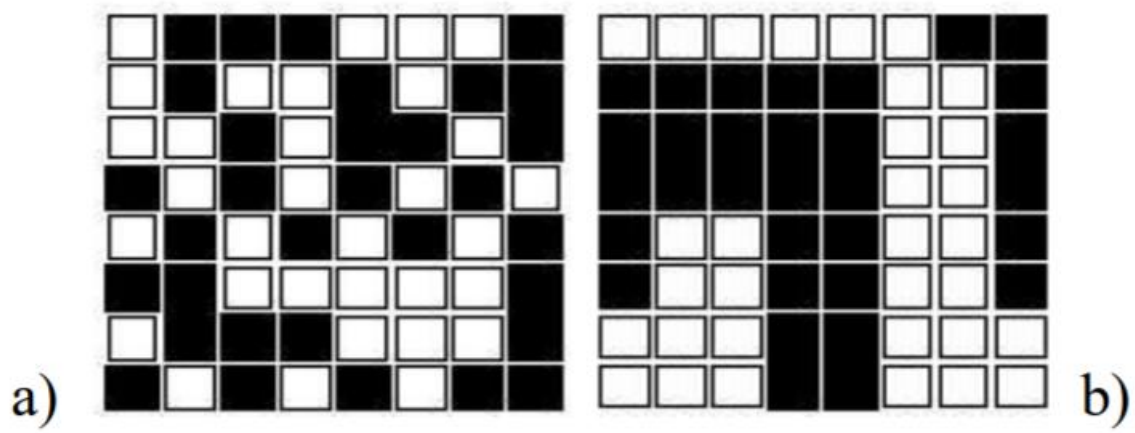
màu trắng (biểu diễn giá trị 1), trong mặt phẳng bit thứ 3 tại vị trí (0,0) có màu đen, tương tự đến mặt phẳng bit thứ 8 tại vị trí (0,0) có màu đen (biểu diễn giá trị 0).



Hình 2.4. Mặt phẳng bit của các điểm ảnh trong khung hình của video.

Trong tài liệu này áp dụng phân đoạn mặt phẳng bit nhiễu cho khung hình với các điểm ảnh 8-bit bằng cách tính toán tỉ lệ nhiễu của từng vùng mặt phẳng bit theo thành phần màu sắc, từ đó có thể xác định tỉ lệ giấu từ 20 – 40 % thông tin vào vùng mà ít ảnh hưởng đến cảm nhận chất lượng ban đầu của khung hình.

Nhiều nghiên cứu chỉ ra rằng thị giác của con người có cảm nhận tốt với các điểm bất thường trong vùng đồng màu nhưng lại kém hiệu quả trong vùng có màu phức tạp. Khi một ảnh được phân giải trong mặt phẳng bit, độ phức tạp của từng vùng mặt phẳng có thể đo được. Các vùng đồng màu sắc hoặc có rất ít thay đổi giá trị giữa bit 0 và 1 sẽ có độ phức tạp thấp, các vùng có độ phức tạp cao như ảnh của một khu rừng xuất hiện nhiều khối nhiễu với nhiều biến đổi giữa bit 0 và 1 và đây là khu vực lý tưởng để giấu tin vì hệ thống thị giác của con người khó phát hiện được sự thay đổi giá trị ở khu vực này. Để hạn chế ảnh hưởng nhiều đến chất lượng ảnh ban đầu người ta chỉ thay đổi mặt phẳng bit có trọng số thấp LSB để giấu tin, đây chính là trường hợp riêng của LSB cổ điển.



Hình 2.5. Khối nhiễu (a) và khối nhiều thông tin (b): (a) sự phức tạp 69, (b) sự phức tạp 29.

Do đó sự phức tạp của tường mặt phẳng bit là số lượng chuyển tiếp canh 1 – 0 và 0-1 theo cả hướng ngang và hướng dọc. Độ phức tạp của từng vùng mặt phẳng bit không phụ thuộc vào số lượng các bit số 0 và 1 một của vùng. Đối với mặt phẳng vuông kích cỡ 2n x 2n thì sự phức tạp có giá trị tối đa là 2 x 2 n (2n-1) và tối thiểu là 0. Ví dụ trong trường hợp vùng mặt phẳng bit kích thước 8 x 8 bit thì độ phức tạp tối đa là 112. Như minh họa trong hình 2.5, khối a) gọi là khối nhiễu và khối b) gọi là khối nhiều thông tin, bằng quan sát ta thấy có cùng số lượng bit 0 và 1 là như nhau nhưng độ phức tạp lại khác nhau. Điều này cho thấy khối a) có rất it thông tin thị giác hơn khối b), do đó nếu biến đổi khối a) để giấu thông tin mật thì có ảnh hưởng rất thấp về chất lượng ảnh. Ngược lại, nếu biến đổi khối b) để giấu thông tin sẽ gây ra biến dạng hay nhòe cạnh nhất định của hình ảnh, do đó sẽ gây ra nghi ngờ ít nhiều. Phương pháp này hoạt động rất tốt đối với khung hình của video tự nhiên vì nó có nhiều vùng nhiễu cao do đó có thể giấu thông tin với tỉ lệ cao. Với các khung hình có vùng bit ít phức tạp thì bất cứ thay đổi nào đều có thể tạo ra các dấu vết rõ ràng.

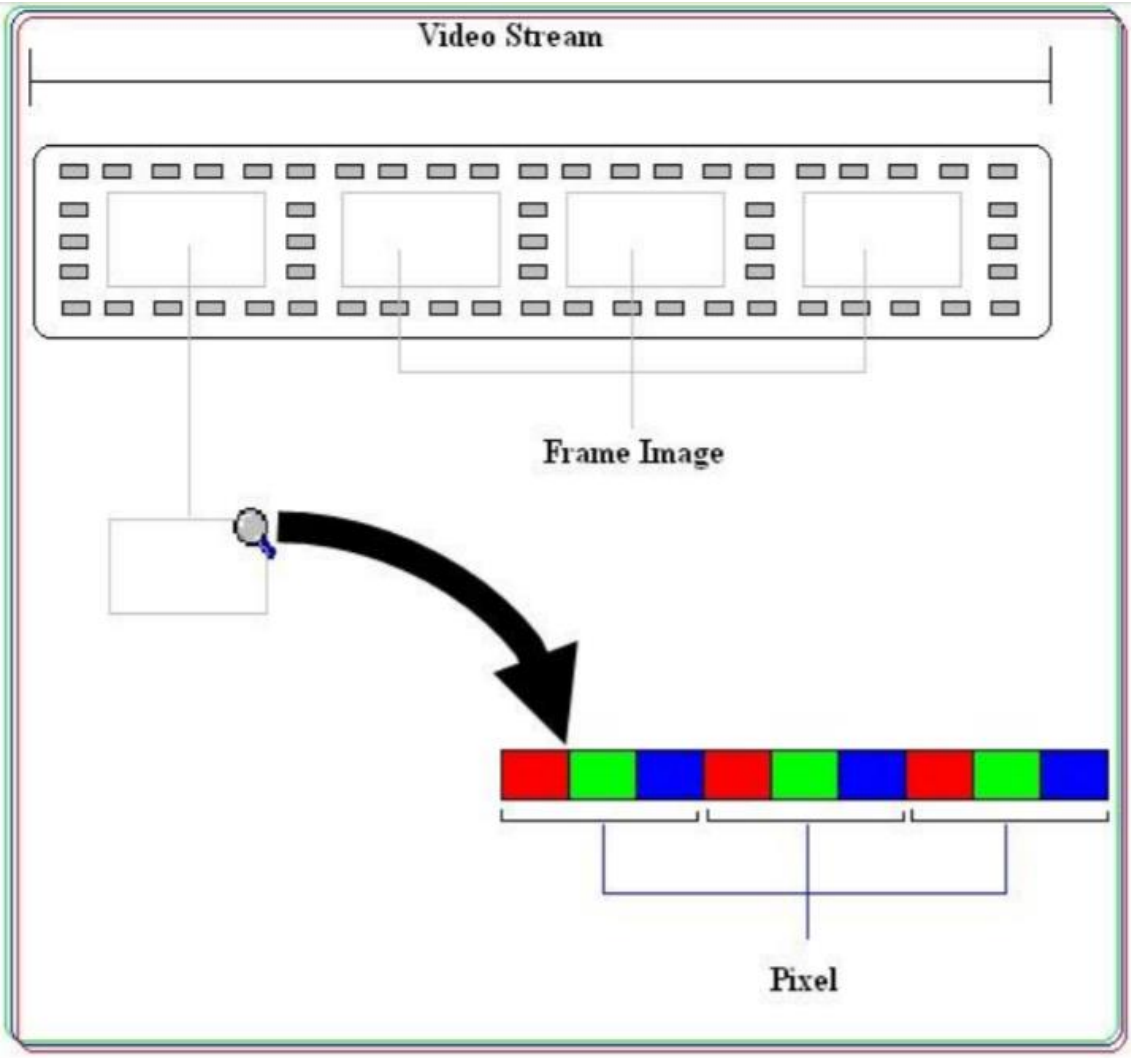
Kỹ thuật giấu tin áp dụng BPCS có thể giấu thông tin với tỉ lệ lên đến 50% kích thước của khung hình. Tuy nhiên cho tới nay chỉ có thể sử dụng tốt với ảnh 24 bit màu, tuy nhiên ở đây chúng ta chỉ minh họa với ảnh 8 –bit màu để đơn giản hóa, khi cài đặt thực tế chúng ta có thể mở rộng tương ứng cho 24 bit màu.

Với ảnh có bằng màu các chỉ số màu trong ảnh được lập chỉ mục không cụ thể, điều này có thể gây ra một vấn đề nghiêm trọng trong việc áp dụng BPCS. Ví dụ trong hình 2.4, thông tin mật nhị phân được nhúng vào mặt phẳng bit ít quan trọng thứ tám, hay với hình 2.5 (a) có ngưỡng phức tạp $\alpha 0=35/112$ để nhúng vào khối nhiễu, dù sự thay đổi mỗi giá trị điểm ảnh trong ví dụ này chỉ trên ít nhất một đơn vị nhưng sẽ có thay đổi rất nhiều trong trật tự của bảng màu ảnh. Vì thế khi áp dụng BPCS cho ảnh có bảng màu, thì các

chỉ số màu nên có chỉ số tương tự, thường thì chúng ta sẽ phải sắp xếp lại bảng màu và trật tự màu tương ứng của khung hình trước khi giấu thông tin.

2.2.1. Quy trình giấu và tách tin sử dụng BPCS.

Khi áp dụng kỹ thuật giấu tin BPCS cho video, chúng ta sẽ thực hiện chọn khung hình nào đó để giấu tin (có thể một hoặc nhiều khung hình tùy thuộc vào độ dài của thông tin mật), như minh họa trong hình 2.6, tách khung hình ra khỏi video, cụ thể được trình bày như sau:



Hình 2.6. Tách khung hình từ tệp Video

. • Đọc khung hình.

• Chọn Khung hình.

• Che giấu thông tin mật.

• Đọc các khung hình liên tục.

• Trích xuất dữ liệu

Hình trên cho thấy khung được chọn với hoạt động giấu khung này linh hoạt hơn để chỉ định điểm bắt đầu của khung cũng như các điểm kết thúc, tính năng mới này làm cho hệ thống an toàn hơn về mặt tránh phát hiện các dữ liệu giấu bằng cách sử dụng kỹ thuật thống kê.

Độ phức tạp alpha cho một vùng khung hình nhị phân kích thước m x m được định nghĩa như sau:

$$\alpha = \frac{k}{2m(m-1)}, \quad 0 \leq \alpha \leq 1$$

(2.1)

Với k là tổng các đường viền giữa màu đen và trắng trong ảnh và 2m (m-1) là chiều dài biên tối đa có thể thu được từ một mẫu m x m.

Các bước thực hiện giấu tin sử dụng BPCS:

Bước 1: Chia từng vùng ảnh thành các mặt phẳng bit với kích thước 8 × 8. Phân loại các vùng thành các vùng "nhiều thông tin" và "nhiễu" dựa trên ngưỡng phân loại α0.

Bước 2: Nhúng thông tin vào các "nhiễu" để tạo thành vùng có giấu tin. Mỗi vùng này được coi là ảnh nhị phân kích cỡ 8 × 8.

Bước 3: Nếu một khối bí mật ít phức tạp hơn so với ngưỡng α0, liên hợp chúng để làm cho nó có giá trị độ phức tạp cao..

Bước 4: Nhúng từng khối bí mật vào vị trí các khối nhiễu của mặt phẳng bit. Nếu khối này được liên hợp thì ghi lại sự kiện này trong một bản đồ định vị (location map).

Bước 5: Có thể nhúng bản đồ định vị vùng giấu tin cùng các khối bí mật hoặc lưu trữ riêng.

2.3.Giấu tin trên âm thanh của video

2.3.1. Giấu trên LSB của âm thanh video

Thuật toán giấu tin và tách tin trên k bit LSB của tín hiệu âm thanh video được trình bày chi tiết dưới đây.

Thuật toán giấu tin:

Đầu vào: Audio gốc A có độ dài tín hiệu L, chuỗi tin cần giấu M.

Đầu ra: Audio đã giấu tin.

Các bước thực hiện:

Bước 1: Đọc audio vào A, dựa vào tần số lấy mẫu và các thông số liên quan đến cấu trúc lưu trữ của tệp audio ta được vector giá trị của tín hiệu mẫu lưu vào mảng một chiều để thực hiện giấu tin.

Bước 2: Thực hiện chuyển đổi chuỗi tin cần giấu M sang chuỗi bit nhị phân để có thể giấu vào audio, tính độ dài số bit thông điệp lưu vào L.

Bước 3: Chọn giá trị k phù hợp nhất (tức là chọn số bit LSB của tín hiệu audio sẽ giấu tin)

Bước 4. Dựa vào k được chọn ở bước 3, thực hiện giấu L (độ dài bit thông điệp) vào LSB của ba tín hiệu đầu tiên hoặc cuối cùng của tín hiệu audio để phục vụ tách tin.

Bước 5: Dựa vào k đã chọn và độ dài L của thông điệp ta thực hiện chia chuỗi bit thông điệp thành các chuỗi con có độ dài k bit. Mỗi chuỗi con này sẽ được thay thế vào k bit LSB của L/k tín hiệu audio để có thể giấu đủ L bit thông điệp.

Bước 6: Lưu lại các tín hiệu audio vào tệp audio kết quả ta được audio đã giấu tin S.

Thuật toán tách tin:

Đầu vào: Audio đã giấu tin S.

Đầu ra: Thông điệp đã giấu M.

Các bước thực hiện:

Bước 1: Đọc audio vào S, dựa vào tần số lấy mẫu và các thông số liên quan đến cấu trúc lưu trữ của tệp audio ta được vector giá trị của tín hiệu mẫu lưu vào mảng một chiều để thực hiện tách tin.

Bước 2: Cho biết giá trị k (số bit LSB đã giấu tin).

Bước 3: Tách ra độ dài bit L đã giấu trên ba tín hiệu đầu tiên hoặc cuối cùng của tín hiệu audio.

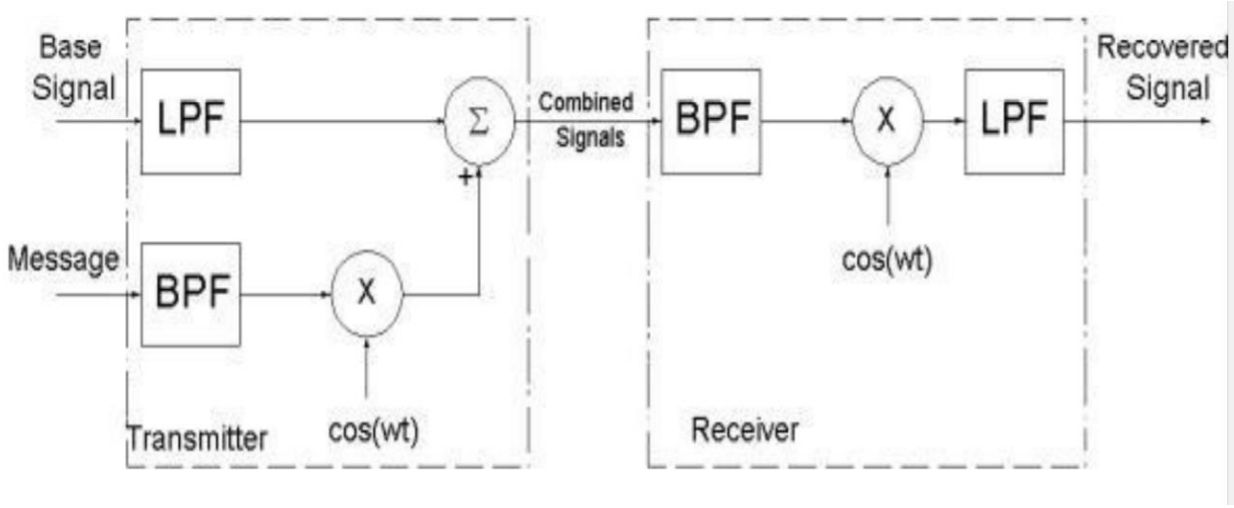
Bước 4: Thực hiện tách k bit LSB của L/k tín hiệu đã giấu tin ghép lại thành chuỗi bit, ta được chuỗi bit đã giấu.

Bước 5: Chuyển đổi chuỗi bit đã tách về dạng ban đầu ta được thông điệp cần tách. Thông điệp ban đầu cần giấu có thể là văn bản, dữ liệu ảnh hoặc là một đoạn audio nào đó.

2.3.2. Giấu tin trên miền biến đổi Fourier của tín hiệu âm thanh video

Đây là kỹ thuật do nhóm tác giả C.J. Ganier, Randall Holman, Julie Rosser và Erik Swanson đề xuất. Theo nhóm tác giả này thì hệ thống thính giác của người trưởng thành có thể phân biệt được tín hiệu âm thanh trong khoảng từ 4kHz đến 18kHz, các tín hiệu thấp nhỏ hơn 4kHz tai người khó có thể nhận biết. Trong thực tế các tín hiệu thấp nhỏ hơn 4kHz không "được sử dụng", do đó nhóm tác giả sử dụng tín hiệu này để nhúng thủy vân [9].

Kỹ thuật thủy vân số trên miền biến đổi là phương pháp thay vì giấu trực tiếp trên các tín hiệu miền thời gian thực thì các tín hiệu sẽ được biến đổi sang miền tần số sau đó mới chèn thông tin cần giấu vào. Tổng quát của phương pháp có thể mô tả qua sơ đồ trong hình 2.8. Hình 2.8.



Sơ đồ tổng quát giấu tin và tách tin trên miền tần số [9]

Theo sơ đồ 2.8 thì tín hiệu vào dùng để che giấu thông tin gọi là tín hiệu cơ sở (Base Signals), tín hiệu sau khi đã giấu thông tin gọi là tín hiệu mang tin (Combined Signals). Bộ LPF (low pass filter) là bộ lọc thông thấp, là bộ lọc chỉ cho thành phần tần số thấp hơn tần số cắt đi qua, thành phần tần số cao thì bị loại bỏ, BPF (Band pass filter) là bộ lọc thông dải, là bộ lọc chỉ cho các thành phần có tần số trong một dải đi qua, các thành phần bé hơn và lớn hơn thì loại bỏ. Bộ cos(wt) là bộ điều chỉnh tín hiệu sử dụng phép toán cosine. Bộ $\sum$ là bộ kết hợp tín hiệu cơ sở với tín hiệu thông điệp.

Quy trình giấu tin được mô tả tóm tắt như sau: giả sử có tín hiệu vào để che giấu thông tin (gọi là tín hiệu cơ sở) và thông điệp (giả sử cũng là một đoạn tín hiệu audio nào đó) cần được che giấu. Sử dụng biến đổi tần số Fourier cho hai tín hiệu này, ta được miền biến đổi Fourier.

Tiếp theo chúng ta thực hiện lọc sử dụng bộ lọc thông thấp LPF đến 18kHz cho tín hiệu cơ sở, sẽ loại bỏ trên 4kHz. Sử dụng bộ lọc thông giải BPF cho tín hiệu thông điệp với giải lọc từ 300Hz đến 3.3 kHz.

Cuối cùng chúng ta thực hiện điều chỉnh tín hiệu thông điệp (đã lọc) sử dụng biến đổi cosine với tần số mang 20kHz. Kết hợp tín hiệu cơ sở (đã lọc) với tín hiệu thông điệp sau khi điều chỉnh chúng ta nhận được tín hiệu mới có giấu thông tin.

Quá trình tách tin được thực hiện ngược lại, sử dụng lọc thông giải BPF cho tín hiệu đã mang tin để tách ra giải thông của tin hiệu thông điệp đã gộp trong tin hiệu cơ sở. Kết quả sau bộ lọc BPF sẽ được điều chỉnh sử dụng bộ cos(wt) bằng phép cosine ta được tín hiệu sau điều chỉnh, tín hiệu này sẽ được sử dụng bộ lọc thông thấp LPF để được tín hiệu thông điệp đã giấu.

Thuật toán giấu tin và tách tin trên miền biến đổi như trình bày sau đây.

Thuật toán giấu tin:

Đầu vào: Audio gốc A có độ dài tín hiệu L, audio cần giấu M.

Đầu ra: Audio đã giấu tin.

Các bước thực hiện:

Bước 1: Đọc audio vào A, dựa vào tần số lấy mẫu và các thông số liên quan đến cấu trúc lưu trữ của tệp audio ta được vector giá trị của tín hiệu mẫu, biến đổi Fourier cho tin hiệu vào (không biến đổi 3 tín hiệu audio cuối cùng để giấu độ dài thông điệp)

Bước 2: Đọc audio cần giấu M, tính độ dài số tín hiệu của M được giá trị L, lưu vào 3 tín hiệu cuối cùng của audio vào A để có thể tách ra M trong quá trình tách tin. Thực hiện biến đổi Fourier cho tin hiệu thông điệp M.

Bước 3: Thực hiện lọc sử dụng bộ lọc thông thấp LPF đến 18kHz cho tín hiệu cơ sở.
Bước 4: Sử dụng bộ lọc thông giải BPF cho tín hiệu thông điệp với giải lọc từ 300Hz đến 3.3 kHz.

Bước 5: thực hiện điều chỉnh tín hiệu thông điệp (đã lọc) sử dụng biến đổi cosine với tần số mang 20kHz. Kết hợp tín hiệu cơ sở (đã lọc) với tín hiệu thông điệp sau khi điều chỉnh chúng ta nhận được tín hiệu mới có giấu thông tin.

Bước 6: Lưu lại các tín hiệu audio đã giấu tin vào tệp audio kết quả ta được audio đã giấu tin S.

Thuật toán tách tin:

Đầu vào: Audio đã giấu tin S.

Đầu ra: Audio thông điệp đã giấu M.

Các bước thực hiện:

Bước 1: Đọc audio vào S, dựa vào tần số lấy mẫu và các thông số liên quan đến cấu trúc lưu trữ của tệp audio ta được vector giá trị của tín hiệu để thực hiện tách tin.

Bước 2: Tách ra độ dài tín hiệu L đã giấu trên ba tín hiệu đầu tiên hoặc cuối cùng của tín hiệu audio.

Bước 3: Sử dụng lọc thông giải BPF cho tín hiệu đã mang tin để tách ra giải thông của tin hiệu thông điệp đã giấu.

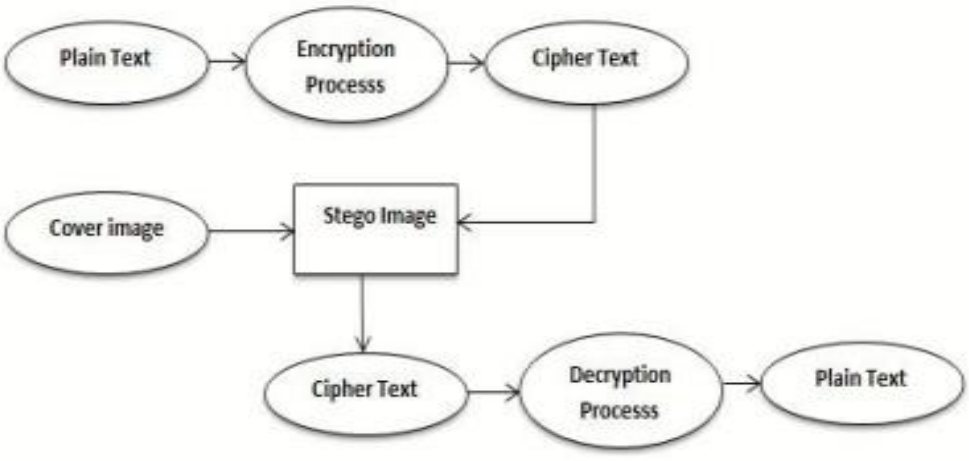
Bước 4: Điều chỉnh tín hiệu sử dụng bộ cos(wt) bằng phép cosine ta được tín hiệu sau điều chỉnh, tín hiệu này sẽ được sử dụng bộ lọc thông thấp LPF ta được tín hiệu thông điệp đã giấu.

Bước 5: Kết hợp với độ dài tín hiệu L đã giấu ta được audio thông điệp. Thuật toán trong kỹ thuận này phù hợp với phương pháp thủy vân số dùng để giấu một đoạn audio vào audio cơ sở mục đích bảo vệ bản quyền số đối với dữ liệu âm thanh.

Chương 6: Các ứng dụng của steganography

Ứng dụng steganography, ngày nay, nhiều nước phát triển, chữ kí tay đã được số hóa và lưu trữ, được sử dụng như là hồ sơ các nhân của các dịch vụ ngân hàng và tài chính, nó được dùng để xác thực trong các giao dịch thẻ tín dụng của người tiêu dùng.

Sự kết hợp của Steganography và Cryptography làm tăng tính bảo mật cho việc truyền thông bí mật.



Hình 8 : Mô hình kết hợp giữa Steganography và Cryptography[8]

CHƯƠNG 7 DEMO

Demo cho kỹ thuật giấu tin trong ảnh bằng thuật toán LSB (Thay thế bit cuối cùng)

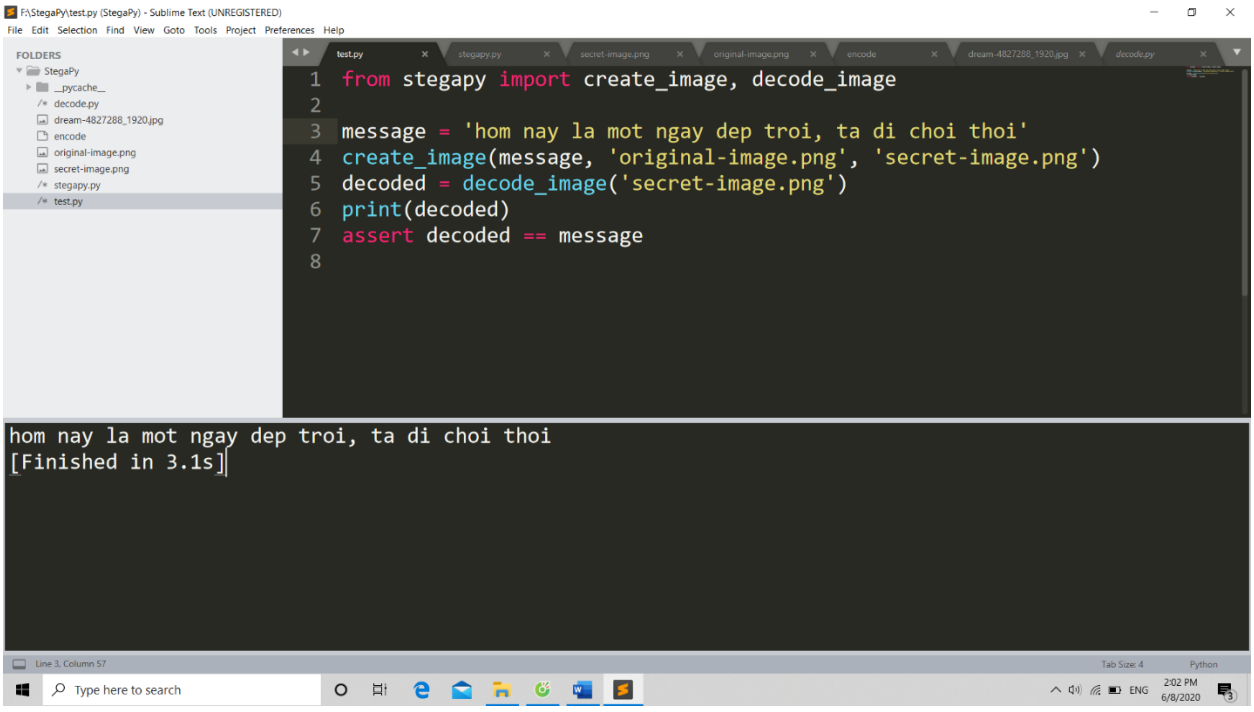
Input: Ảnh và thông điệp

Output: Ảnh chứa thông điệp

Môi trường lập trình: Python

Figure 1. Cover image

Figure 2. Stego image



KẾT LUẬN

Trong bài báo cáo này, nhóm chúng em đã tìm hiểu và phân tích các kỹ thuật giấu tin đa phương tiện (text, hình ảnh, audio và video). Trong thời gian tới nhóm sẽ tiếp tục tìm hiểu các kỹ thuật khác tối ưu hơn.

Danh mục tài liệu tham khảo

1. *Steganography An Art of Hiding Data*, Shashikala Channalli et al /International Journal on Computer Science and Engineering Vol.1(3), 2009, 137-141.
2. *Steganography and Steganalysis: Different Approaches*, Soumyendu Das Information Security Consultant, Kolkata, India, soumyendu.das@gmail.com Subhendu Das, STQC IT Services, Kolkata, India, subhendu.das@gmail.com Bijoy Bandyopadhyay, Institute of Radio physics & Electronics, University of Calcutta, Kolkata, India, bbandy@vsnl.com, Sugata Sanyal, Tata Institute of Fundamental Research, Mumbai, India, sanyal@tifr.res.in
3. *Text Steganography*, Shikha Vidhu Kiran Dutt, M.tech Dept of CSE, JCDV Sirsa & GJU LECT in Dept of CSE, JCDV Sirsa & GJU, Hissar, India Hissar, India, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 10, October 2014.
4. *TEXT STEGANOGRAPHIC APPROACHES: A COMPARISON*, Monika Agarwal, Department of Computer Science and Engineering, PDPM-IIITDM, Jabalpur, India, International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.1, January 2013.
5. *Robust text watermarking based on line shifting*, Alexander Kozachok, Sergey Kopylov.
6. *A Novel Image Steganographic Approach for Hiding Text in Color Images using HSI Color Model*, *Khan Muhammad, Jamil Ahmad, Haleem Farman, Muhammad Zubair, Department of Computer Science, Islamia College Peshawar, Pakistan
7. *Image Steganography Techniques*, Ravi K Sheth, Assistant Professor (IT), Raksha Shakti University, Ahmedabad, Rashmi M. Tank, M.E.(C.E.), student, B.V.M.Engineering College, V V Nagar, International Journal of Computer Engineering and Sciences(IJCES) Volume-1 Issue-2, 2015
8. *A Survey on different techniques of steganography*, Harpreet Kaur and Jyoti Rani, CSE Department, GZSCCET Bathinda, Punjab, India, MATEC Web of Conferences 57, 02003 (2016) ICAET 2016 (Pathak & Bhuyar, 2014)
9. *Nhập môn xử lý ảnh số, Lương Mạnh Bá, Nguyễn Thu Thủy, NXB khoa học và kỹ thuật Hà Nội 2003.*
10. *Nghiên cứu kỹ thuật giấu tin trong audio hỗ trợ xác thực, Nguyễn Xuân Huy, Huỳnh Bá Diệu, Viện Công nghệ thông tin, Viện Khoa học Công nghệ Việt Nam, 18 Hoàng Quốc Việt, Hà Nội, Việt Nam, Khoa Công nghệ thông tin, Trường đại học Công nghệ, ĐHQGHN, 144 Xuân Thuỷ, Hà Nội, Việt Nam, Nhận ngày 26 tháng 12 năm 2008.*
11. *Một số kỹ thuật giấu tin trong âm thanh số, Huỳnh bá Diệu, Luận án tiến sĩ hệ thống thông tin trường Đại học Công nghệ, Đại học Quốc gia Hà Nội 2017.*