HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

ĐỖ XUÂN CHỢ

GIÁO TRÌNH

CÁC KỸ THUẬT GIẤU TIN

Hà Nội, tháng 5 năm 2023

MỞ ĐẦU

Giấu tin là một trong các kỹ thuật đã ra đời và phát triển từ lâu. Nếu như trước kia việc triển khai và áp dụng các kỹ thuật giấu tin thường được sử dụng trong lĩnh vực quân sự, quốc phòng thì ngày nay các ứng dụng của giấu tin được triển khai và áp dụng ở hầu hết trong các lĩnh vực và công nghệ trong đời sống. Chính vì những lợi ích to lớn của lĩnh vực giấu tin mang lại mà hiện nay mỗi công ty, doanh nghiệp, tổ chức hoặc rộng hơn là quốc gia đều có những nghiên cứu và ứng dụng kỹ thuật giấu tin để phục vụ cho lợi ích của mình.

Môn học "Các kỹ thuật giấu tin" là môn chuyên ngành thuộc chương trình đào tạo đại học ngành An toàn thông tin của Học Viện Công Nghệ Bưu Chính Viễn Thông. Môn học cung cấp các kiến thức liên quan đến lĩnh vực giấu tin bao gồm: tổng quan về các kỹ thuật giấu tin; một số phương pháp giấu tin trong môi trường đa phương tiện; một số ứng dụng của các kỹ thuật giấu tin đang được triển khai trong thực tế.

Giáo trình "Các kỹ thuật giấu tin" được biên soạn trên cơ sở đề cương chi tiết môn học đã được duyệt và tổng hợp tài liệu từ nhiều nguồn tin cậy nhằm cung cấp tài liệu phục vụ cho sinh viên, học viên thạc sỹ nghiên cứu và học tập. Giáo trình được cấu trúc thành các chương như sau:

Chương 1: Tổng quan về kỹ thuật giấu tin. Chương này cung cấp các kiến thức cơ bản liên quan đến kỹ thuật giấu tin bao gồm: khái niệm, các thuật ngữ, phân loại, một số ứng dụng cơ bản…. Bên cạnh đó, trong chương này giáo trình còn trình bày một số khái niệm, phân loại về tấn công vào kỹ thuật giấu tin.

Chương 2: Giấu tin trong ảnh. Chương 2 sẽ đi sâu vào trình bày và phân tích đặc điểm, yêu cầu đối với các kỹ thuật giấu tin trong ảnh. Bên cạnh đó hai phương pháp chính được áp dụng để giấu tin trong ảnh là giấu tin trong miền không gian và giấu tin trong miền tần số cũng sẽ được giáo trình mô tả chi tiết trong chương này.

Chương 3: Giấu tin trong âm thanh. Trong chương này, trước tiên giáo trình sẽ mô tả một số định dạng của các file âm thanh và đặc điểm của chúng. Trên cơ sở đó, các nội dung về kỹ thuật giấu tin và tách tin trong âm thanh bao gồm: khái niệm, đặc điểm, nguyên tắc giấu tin và tách tin, đánh giá ưu điểm và nhược điểm của kỹ thuật giấu tin trong âm thanh sẽ được giáo trình trình bày chi tiết.

Chương 4: Giấu tin trong video. Nội dung của chương 4 sẽ tập trung vào hai vấn đề chính. Theo đó, phần đầu của chương, giáo trình sẽ liệt kê và phân tích một số định dạng file video phổ biến hiện nay. Tiếp theo sẽ trình bày về đặc điểm và quy trình của một số phương pháp giấu tin và tách tin trong video. Bên cạnh đó, đối mỗi phương pháp giấu tin, giáo trình có những phân tích và đánh giá về ưu điểm, nhược điểm của chúng từ đó cung cấp cho người đọc cơ chế lựa chọn các kỹ thuật giấu tin cho phù hợp với nhu cầu sử dụng của mình.

Giáo trình Các kỹ thuật giấu tin được biên soạn và chỉnh sửa dựa trên kinh nghiệm của tác giả trong quá trình giảng dạy và nghiên cứu môn học này tại Học Viện Công Nghệ

Bưu Chính Viễn Thông. Bên cạnh đó, tác giả cũng thu thập ý kiến phản hồi của đồng nghiệp và sinh viên theo các từng khóa để bổ sung và cập nhật các kiến thức, nội dung sao cho phù hợp nhất với đối tượng người học. Giáo trình này có thể được sử dụng làm tài liệu tham khảo cho sinh viên, học viên thạc sỹ ngành An toàn thông tin cũng như ngành Công nghệ thông tin. Trong quá trình biên soạn, mặc dù đã cố gắng, song giáo trình sẽ khó tránh khỏi những thiếu sót. Tác giả mong nhận được các phản hồi và ý kiến đóng góp của đọc giả để nội dung cuốn sách được hoàn thiện hơn trong các lần tái bản tiếp theo. Cuối cùng, tác giả gửi lời cảm ơn chân thành đến các đồng nghiệp, các thế hệ sinh viên ngành An toàn thông tin đã có những ý kiến đóng góp ý nghĩa để tác giả hoàn thiện cuốn sách này.

Hà nội, tháng 5 năm 2023

Tác giả

MỤC LỤC

DANH MỤC CÁC TỪ VIẾT TẮT

Từ viết tắt	Thuật ngữ Tiếng Anh	Thuật ngữ Tiếng Việt
LSB	Least Significant Bit	Bit có trọng số thấp nhất
DCT	Discrete Cosine Transformations	Chuyển đổi cosin rời rạc
DWT	Discrete Wavelet Transform	Chuyển đổi Wavelet rời rạc
DFT -	Discrete Fourier Transform	Chuyển đổi Fourier rời rạc
DC	DC-coefficient	Hệ số DC
AC	AC-coefficient	Hệ số AC
DSSS	Direct Sequence Spread Spectrum	Trải phổ dãy trực tiếp
FHSS	Frequency Hopping Spread Spectrum	Trải phổ nhảy tần
MPEG	Moving Picture Experts Group	Moving Picture Experts Group
HAS	Human Auditory System	Hệ thống thính giác con người

DANH MỤC CÁC BẢNG BIỂU

DANH MỤC CÁC HÌNH VẼ

CHƯƠNG 1: TỔNG QUAN VỀ KỸ THUẬT GIẤU TIN

1.1. Định nghĩa và khái niệm cơ bản

1.1.1. Giới thiệu chung

Giấu tin (Information Hiding) là ngành khoa học chuyên nghiên cứu về các phương pháp, thuật toán nhằm giấu thông tin vào một đối tượng dữ liệu khác. Cụ thể, những thông tin sẽ được giấu vào trong một đối tượng dữ liệu khác sao cho sự biến đổi của môi trường sau khi giấu là khó nhận biết, đồng thời có thể lấy lại được các thông tin giấu khi cần một cách dễ dàng.

Kỹ thuật giấu tin là quá trình áp dụng các phương pháp, thuật toán nhằm giấu thông tin vào một đối tượng khác. Trong mỗi hệ thống giấu tin sẽ đều có 2 quá trình chính là giấu tin và tách tin. Trong đó:

- *Quá trình giấu tin* là quá trình mà người giấu tin sẽ sử dụng các kỹ thuật phân tích và biến đổi để có thể giấu được thông tin vào đối tượng dữ liệu khác. Theo tài liệu [1] quá trình giấu tin thường sẽ được chia thành 2 giai đoạn chính bao gồm: giai đoạn tiền xử lý dữ liệu và giai đoạn giấu tin vào đối tượng dữ liệu khác.

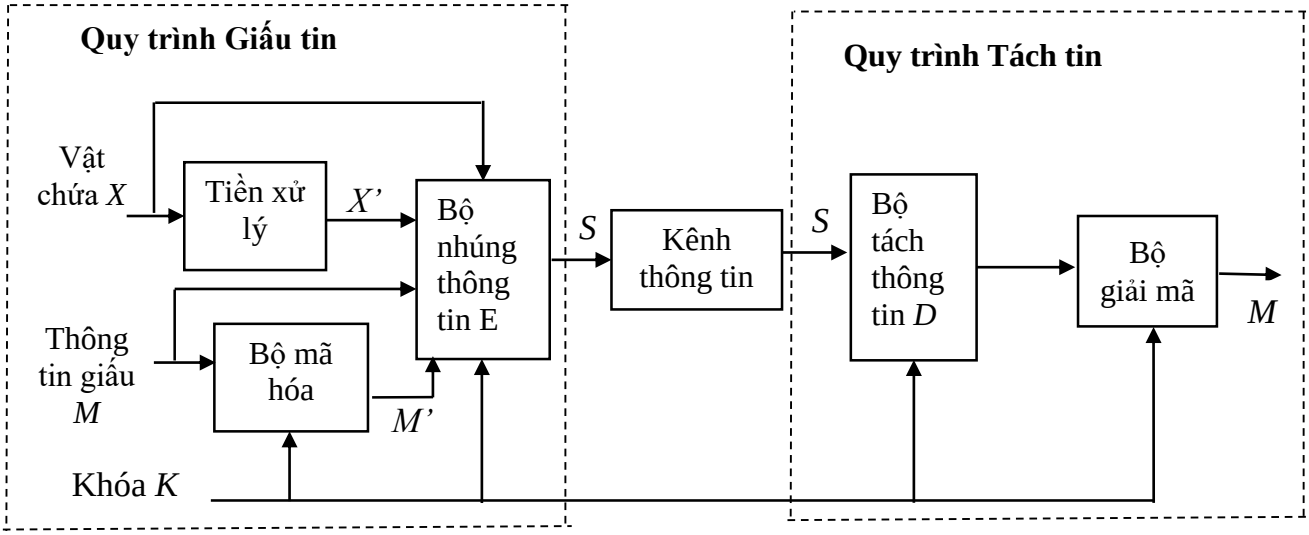
- *Quá trình tách tin* được cho là ngược lại với quá trình giấu tin. Theo đó, người tách tin sẽ tìm cách trích xuất thông tin được giấu trong vật chứa dựa trên các phương pháp và kỹ thuật xử lý dữ liệu khác nhau. Để tách tin thành công, người giấu tin và tách tin cần phải có một số quy ước và thỏa thuận trước như: vị trí giấu tin, vật chứa tin...

Hiện nay các kỹ thuật giấu tin đang được chia thành hai lĩnh vực chính bao gồm: giấu tin mật (Steganography) và thủy vân số (Watermarking). Trong thực tế, hai lĩnh vực này sẽ có các yêu cầu về kỹ thuật, quy trình đối với thông tin cần giấu và đối tượng dữ liệu chứa tin giấu khác nhau. Cụ thể, giấu tin mật sẽ cố gắng đảm bảo việc giữ bí mật cho thông tin cần giấu. Còn thủy vân số thì bảo vệ đối tượng chứa tin giấu.

Từ các định nghĩa và khái niệm về giấu tin có thể dễ dàng nhận thấy rằng, giấu tin có nhiều điểm tương đồng so với mã hóa. Trong thực tế, đã có một số ứng dụng được triển khai bằng cách kết hợp các phương pháp giấu tin với các phương pháp mã hóa. Cụ thể, có thể sử dụng các phương pháp mã hóa để mã hóa thông tin cần giấu trước khi giấu chúng vào đối tượng dữ liệu khác. Cũng có ứng dụng sẽ sử dụng các kỹ thuật giấu tin để vận chuyển và che giấu các thông tin bí mật. Việc sử dụng kết hợp các kỹ thuật giấu tin và kỹ thuật mã hóa đang được coi là một trong những xu thế trong ngành an toàn thông tin. Bởi vì kết hợp hai phương pháp này sẽ khai thác được các ưu điểm của của chúng từ đó nâng cao được hiệu quả ứng dụng.

1.1.2. Một số thuật ngữ cơ bản

Hình 1.1 mô tả mô hình tổng quát của quá trình giấu tin và tách tin phổ biến [1].



Hình 1.1. Mô hình tổng quát quá trình giấu và tách tin

Từ hình 1.1 có thể thấy các tham số chính trong mô hình giấu tin và tách tin bao gồm {*X, M, S, K, E, D*} [1]. Cụ thể:

- *X là vật chứa thông tin*. Theo đó, vật chứa thông tin là các đối tượng được dùng làm môi trường để giấu tin như ảnh, âm thanh, video, văn bản, …
- *M là thông tin cần giấu*. Trong thực tế thông tin *M* chọn tùy theo mục đích của người sử dụng, nó có thể là thông tin (với các tin bí mật) hay các logo, hình ảnh bản quyền (thủy vân), ...
- *K là khóa* (có thể sử dụng hoặc không sử dụng). Trong quá trình giấu và tách tin có thể sử dụng nhiều hơn một khóa. Khóa là một chuỗi ngẫu nhiên được sinh ra bởi bộ sinh số mật mã an toàn (bộ sinh số này đáp ứng một số yêu cầu nhất định). Các số được sinh ra bởi bộ sinh số này có thể xác định vị trí các mẫu đã sửa đổi. Thông tin *M* sẽ được giấu một cách phù hợp với khóa trong các mẫu này do đó vật chứa sẽ ít bị biến dạng.
- *Bộ mã hóa*: là một thiết bị được thiết kế để chuyển đổi thông tin cần giấu *M* sang một hình thức thuận tiện để giấu vào vật chứa. Trước khi giấu thông tin *M* vào vật chứa *X*, cần phải chuyển đổi *M* sang một dạng phù hợp. Ví dụ: Với *X* là 1 file ảnh thì *M* thường phải được biểu diễn dưới dạng mảng bit 2 chiều. Để tăng tính ổn định (tính chống biến dạng) của *M* thì *M* phải được mã hóa chống nhiễu hoặc sử dụng tín hiệu băng thông rộng. Sử dụng khóa *K* để tăng tính bí mật cho *M*. Đầu ra của bộ mã hóa là thông tin đã mã hóa *M'*.
- *Tiền xử lý*: xác định các đặc thù của hệ thống nhận thức của con người từ đó xác định các vị trí ít quan trọng hoặc khó bị phát hiện trong vật chứa *X* giúp cho việc nhúng *M* vào *X* hiệu quả và ít bị phát hiện hơn. Trong thực tế, bộ tiền xử lý thường áp dụng lên cả thông tin cần giấu và vật chứa.

- *E là bộ nhúng thông tin*. Thông tin sẽ được giấu vào trong vật chứa nhờ một bộ nhúng. Bộ nhúng là những chương trình thực hiện các thuật toán để giấu tin. Quá trình nhúng thông tin là quá trình xử lý $E: X \times M \times K \rightarrow S$. Theo tài liệu [1] thì bộ nhúng E phải bao gồm 2 bước chính là chọn vị trí cần giấu và phương pháp giấu tin vào vị trí đã lựa chọn. Đối với bước lựa chọn vị trí giấu, đây là bước rất quan trọng vì nó quyết định đến sự thành công của mô hình giấu tin. Còn bước giấu tin vào vị trí đã lựa chọn thì người giấu tin sẽ sử dụng một số phương pháp biến đổi phổ biến như thay thế, hoán vị hoặc XOR để giấu tin vào vật chứa.
- *S là đối tượng đã chứa tin*. Về cơ bản *S* là vật chứa *X* và thông tin cần giấu *M*. Về mặt chất lượng *S* không được khác biệt nhiều so với vật chứa *X*.
- *Bộ tách thông tin D*. Quá trình tách tin được thực hiện thông qua một bộ tách tin tương ứng với bộ nhúng thông tin của quá trình nhúng. Bộ tách triển khai các thuật toán tách tin tương ứng với các thuật toán giấu tin. Trong kỹ thuật giấu tin thì bộ tách thông tin cũng quan trọng không kém so với bộ nhúng thông tin. Bộ tách thông tin cũng sử dụng các phương pháp, thuật toán, kỹ thuật nhằm tìm kiếm và trích xuất thông tin. Thông thường thì mỗi kỹ thuật giấu tin thì sẽ có kỹ thuật tách tin tương ứng. Quá trình tách thông tin là quá trình xử lý $D: S \times K \rightarrow M, X$.
- *Bộ giải mã*: dùng để phục hồi thông tin được giấu *M*. Bộ này có thể sử dụng hoặc không tùy thuộc vào quá trình giấu tin có sử dụng kỹ thêm các kỹ thuật mã hóa hay không.

1.1.3. Các yêu cầu đối với kỹ thuật giấu tin

Một hệ thống giấu tin cần đảm bảo được các yêu cầu sau [1, 2]:

- **Tính vô hình**: tính vô hình của kỹ thuật giấu tin thể hiện ở điểm thông tin giấu khó có khả năng bị phát hiện bằng các hệ thống trực giác bình thường. Trong kỹ thuật giấu tin, các thông tin cần giấu sẽ được giấu vào vật chứa. Chính vì vậy, sau khi thông tin được giấu vào vật chứa thì chắc chắn sẽ có ít hoặc nhiều thay đổi đối với vật chứa đó. Vấn đề đặt ra là làm thế nào để thông tin này có thể trở nên vô hình trong vật chứa. Tùy theo mức độ bảo mật cũng như ứng dụng của kỹ thuật giấu tin mà có các yêu cầu riêng đối với tính vô hình. Ngoài ra, tính vô hình của thông tin trong vật chứa cũng được định nghĩa và xác định khác nhau tùy theo môi trường chứa tin. Ví dụ: tính vô hình của các kỹ thuật giấu tin trong ảnh thể hiện ở việc không nhìn thấy, không phân biệt được sự khác nhau giữa ảnh gốc và ảnh chứa tin giấu. Đối với phương pháp giấu tin trong âm thanh, tính vô hình thể hiện ở chỗ không phân biệt được sự khác nhau khi nghe tệp âm thanh gốc và tệp âm thanh chứa tin. Một kỹ thuật giấu tin tốt sẽ cần phải khai thác các đặc điểm, cấu trúc và định dạng của vật chứa để giấu tin sao cho thông tin trở nên vô hình nhất trong vật chứa.
- **Tính bền vững**: Sau khi giấu thông tin vào vật chứa, bản thân chính những vật chứa tin đó có thể phải trải qua các khâu biến đổi khác nhau. Không giống như kỹ thuật mã hóa, trong một số ứng dụng kỹ thuật giấu tin có những ứng dụng mà thông tin cần giấu không cần thiết phải bí mật nhưng lại rất cần sự toàn vẹn. Chính vì vậy, tính bền vững là thước đo sự nguyên vẹn của thông tin được giấu sau những biến đổi đó.

- **Tính bí mật**: Tính bí mật trong kỹ thuật giấu tin thể hiện ở mức độ ẩn thông tin trong vật chứa. Các phương pháp giấu thông tin phải cung cấp chức năng bảo mật cho dữ liệu sao cho chỉ có người sử dụng hợp lệ mới có thể truy cập vào nó, người dùng bất hợp pháp không thể phát hiện hay đọc được thông tin được giấu. Điều này rất quan trọng để bảo vệ tính bí mật và độ nhạy cảm của thông tin được gửi đi.
- **Dung lượng giấu**: Dung lượng giấu được tính bằng tỷ lệ của thông tin giấu so với kích thước vật chứa. Dung lượng giấu lớn hay nhỏ phụ thuộc vào mục đích giấu tin. Trong thực tế khi thực hiện giấu tin, người giấu tin luôn phải cân nhắc giữa dung lượng và các tiêu chí khác nhau như tính vô hình, tính bền vững...

1.1.4. Lịch sử phát triển

Như đã trình bày ở trên, kỹ thuật giấu tin được phát triển thành hai lĩnh vực chính với những yêu cầu và tính chất khác nhau đó là giấu tin mật và thủy vân số. Trong đó:

- Giấu tin mật chủ yếu phục vụ cho mục đích liên lạc bí mật. Đây là lĩnh vực có lịch sử hình thành và phát triển từ lâu đời, nó bắt nguồn từ Hi Lạp (khoảng năm 440 TCN) và được sử dụng cho tới ngày nay. Theo các tài liệu nghiên cứu tại [3], kỹ thuật giấu tin cổ xưa nhất và cũng là đơn giản nhất là ở thời Hy Lạp cổ đại. Thời kỳ này để gửi thông tin mật đi người gửi dùng các bảng gỗ khắc các thông báo và hình ảnh cần giấu rồi phủ sáp ong lên hoặc xăm tin tức lên đầu của người mang tin, để một thời gian cho tóc mọc lại, rồi lại cạo trọc đi khi muốn đọc bản tin đó. Khi kỹ thuật phát triển hơn, con người sử dụng chữ viết với cỡ chữ nhỏ giấu trong các vật dụng hàng ngày (như các hộp, vali có hai đáy) để chuyển đi, hoặc dùng bồ câu để chuyển thông tin. Sang thế kỷ 17, kỹ thuật giấu tin mật được sử dụng bằng cách đánh dấu vào các kí tự cần thiết trên một văn bản, một bài báo công khai nào đó rồi truyền tới tay người nhận. Về sau này, với việc áp dụng các công nghệ hoá học đã mang lại hiệu quả cao và là thời điểm phát triển mạnh mẽ của lĩnh vực giấu tin. Công nghệ hóa học thường được sử dụng trong thời gian này là mực không màu. Mực không màu là các chất lỏng sản phẩm hữu cơ không màu và hiển thị màu khi gặp điều kiện hoá - lý thích hợp. Ngày nay, do sự bùng nổ của cuộc cách mạng trong lĩnh vực tin học - điện tử - viễn thông cùng với sự phát triển vượt bậc của lĩnh vực xử lý số tín hiệu mà lĩnh vực giấu tin được phát triển mạnh mẽ và đa dạng hơn, đặc biệt là với kỹ thuật dùng các vật chứa là các tệp hình ảnh và âm thanh hay video.

- Thủy vân số: được định nghĩa là việc giấu thông tin mang ý nghĩa bảo vệ tính toàn vẹn của vật chứa. Kỹ thuật thủy vân được phát triển vào cuối thế kỷ 13 tại Ý [3]. Thủy vân được sử dụng lần đầu khi các nhà sản xuất giấy làm các hình mờ chìm trong giấy in để ghi lại thương hiệu giấy và bảo vệ bản quyền nhà sản xuất. Khái niệm thủy vân số cũng xuất phát từ khái niệm thủy vân trên giấy. Năm 1979, Szepanski mô tả một mẫu thông tin số có thể nhúng vào tài liệu nhằm mục đích chống giả mạo. Sau này, Holt và các đồng nghiệp mô tả một phương pháp để nhúng mã định danh vào tín hiệu âm thanh. Năm 1988, Komatsu và Tominaga mới lần đầu tiên sử dụng cụm từ "thủy vân số" và đầu những năm 90 thì thủy vân

số mới thực sự nhận được sự quan tâm của các ngành khoa học [3]. Ngày nay, do những lợi ích to lớn của lĩnh vực này mà kỹ thuật thủy vân số nhận được sự quan tâm từ giới khoa học và các ngành công nghiệp.

1.1.5. Vai trò và tầm quan trọng

Có thể thấy rằng, các ứng dụng của kỹ thuật giấu tin nhằm 2 mục đích chính là giấu tin mật và bảo vệ tính toàn vẹn, hợp pháp của dữ liệu. Để hiểu rõ hơn về tầm quan trọng của kỹ thuật giấu tin trong thực tế, hãy cùng tìm hiểu và phân tích về một số lĩnh vực ứng dụng của giấu tin [1, 2, 3].

a) Trong việc bảo vệ tính toàn vẹn

Nguy cơ vi phạm bản quyền này càng trầm trọng thêm do sự gia tăng các thiết bị ghi kỹ thuật số có dung lượng cao. Với thiết bị ghi âm kỹ thuật số, bài hát và phim có thể được ghi với chất lượng gần như bản gốc. Sử dụng các thiết bị ghi âm và sử dụng Internet để phân phối, người dùng lậu có thể dễ dàng ghi lại và phân phối các tài liệu được bảo vệ bản quyền mà không bồi thường thích hợp cho chủ sở hữu bản quyền. Vì vậy, chủ sở hữu sản phẩm số luôn tìm kiếm các công nghệ bảo vệ bản quyền của mình. Lựa chọn đầu tiên là mật mã: Theo đó, sản phẩm số được mã hóa trước khi gửi và khoá giải mã chỉ được cung cấp cho những người đã mua bản sao hợp pháp của sản phẩm này. Tuy nhiên, mã hóa không thể giúp người bán giám sát cách khách hàng hợp pháp xử lý nội dung sau khi giải mã. Một người dùng lậu có thể mua sản phẩm, sử dụng khóa giải mã để có được một bản sao không được bảo vệ của sản phẩm và sau đó tiến hành phân phối các bản sao bất hợp pháp. Do vậy, chủ sở hữu sản phẩm số cần một công nghệ có thể bảo vệ nội dung ngay cả khi nó được giải mã. Để giải quyết vấn đề này thì lựa chọn kỹ thuật giấu tin với giải pháp thủy vân số là một giải pháp hiệu quả. Thủy vân số được sử dụng vì nó đặt thông tin bản quyền trong sản phẩm mà thông tin bản quyền đó không bao giờ có thể gỡ bỏ được trong quá trình sử dụng bình thường. Thủy vân số có thể được thiết kế để tồn tại sau tất cả các quy trình: giải mã, tái mã hóa, nén, chuyển đổi từ kỹ thuật số sang tương tự và thay đổi định dạng tệp. Trong ngăn ngừa sao chép, thủy vân có thể được sử dụng để thông báo rằng phần mềm này nên hạn chế sao chép. Trong các ứng dụng bảo vệ bản quyền, thủy vân có thể được dùng để xác định chủ sở hữu bản quyền và đảm bảo thanh toán kinh phí hợp lệ.

b) Trong việc truyền thông tin mật

Truyền thông điện tử đang ngày càng nhạy cảm với việc nghe trộm và can thiệp độc hại. Các yêu cầu về tính toàn vẹn, bí mật hoàn toàn có thể được đáp ứng bởi giải pháp sử dụng mã hóa. Tuy nhiên, các kỹ thuật mã hóa trong trường hợp này thường yêu cầu chi phí cao trong việc xây dựng và vận hành. Chính vì vậy, hiện nay kỹ thuật giấu tin đang được lựa chọn cho giải pháp truyền thông tin mật. Việc áp dụng các kỹ thuật giấu tin trong truyền tin mật vẫn đảm bảo các tính chất của an toàn thông tin như:

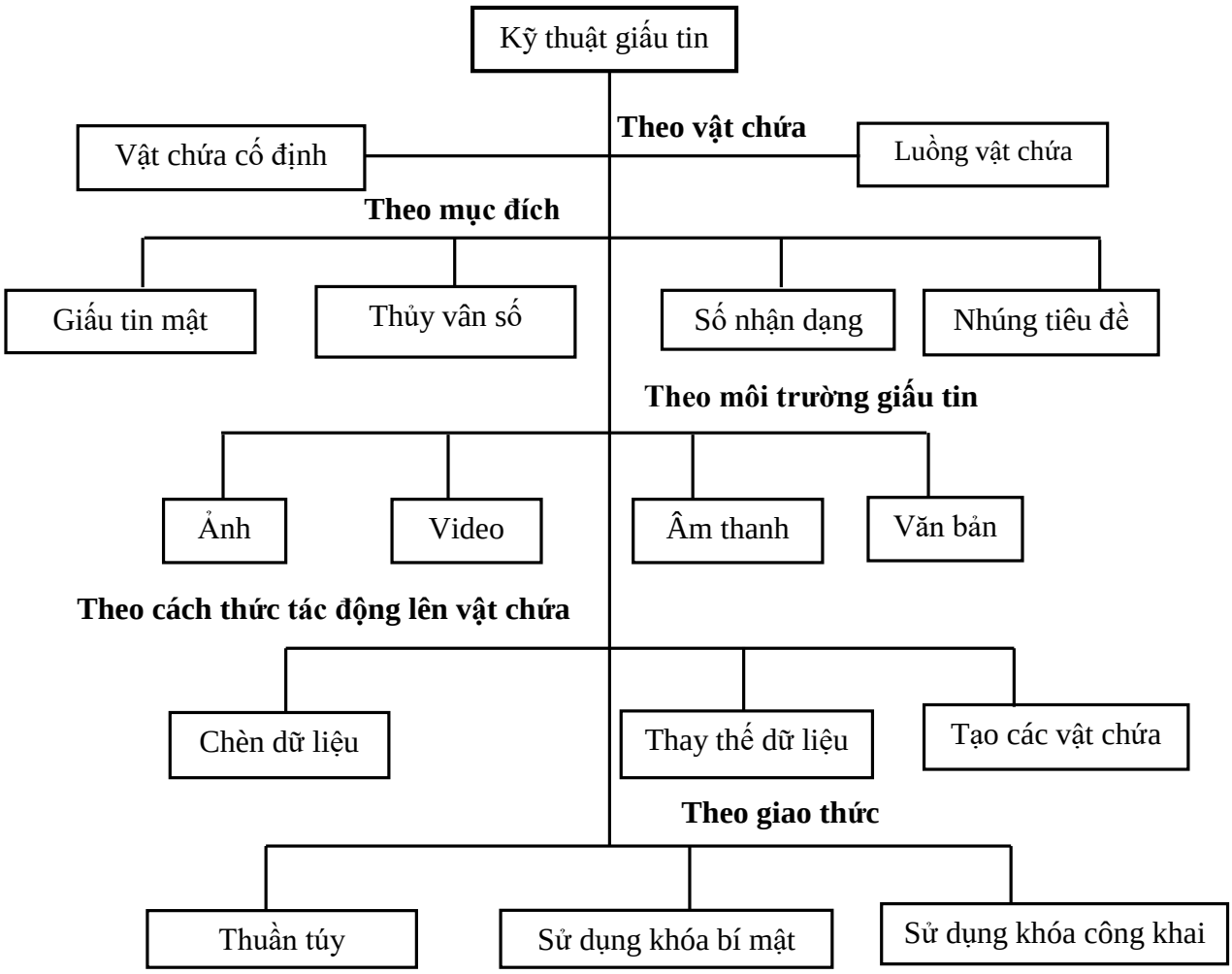
- Tính bí mật (confidentiality): thông tin chỉ được phép truy cập bởi những đối tượng hợp lệ, những đối tượng được cấp phép.

- Tính toàn vẹn thông tin (integrity): đảm bảo thông tin không bị thay đổi trong quá trình truyền tin hay khi có bất kì hành động nào tác động vào vật chứa tin; hoặc nếu có thay đổi thì sẽ bị phát hiện.
- Tính xác thực (authentication): đảm bảo các bên liên quan nhận biết và tin tưởng nhau, đồng thời đảm bảo thông tin trao đổi là thông tin thật.
- Tính chống chối bỏ (non-repudiation): đảm bảo rằng các bên liên quan không thể chối bỏ các hành động đã thực hiện trước đó.

1.2. Phân loại các kỹ thuật giấu tin

1.2.1. Tổng quan về phân loại giấu tin

Trong thực tế kỹ thuật giấu tin nhằm hai mục đích chính là: bảo vệ cho thông tin được giấu trong vật chứa và bảo vệ cho chính vật chứa đó. Do đó sẽ có nhiều phương pháp và tiêu chí khác nhau để có thể phân loại các hướng tiếp cận của các phương pháp giấu tin. Hình 1.2 liệt kê một số cách thức để phân loại kỹ thuật giấu tin.



Hình 1.2. Phân loại các kỹ thuật giấu tin

Từ hình 1.2 có thể thấy kỹ thuật giấu tin rất phong phú và đa dạng. Tùy theo mục đích sử dụng mà người giấu tin có thể lựa chọn phương pháp sao cho phù hợp nhất. Tiếp theo, giáo trình sẽ trình bày chi tiết về đặc điểm của từng phương pháp giấu tin theo cách thức phân loại như hình 1.2.

a) Phân loại theo vật chứa

Trên hình 1.2 có thể thấy các phương pháp giấu tin theo luồng vật chứa sẽ được phân thành 2 nhóm chính là:

- Luồng vật chứa: Luồng vật chứa là các chuỗi bit liên tục. Thông tin được giấu vào trong thời gian thực, vì vậy bộ giấu thông tin không được biết trước kích thước thông tin cần giấu. Một vật chứa lớn có thể giấu được nhiều thông tin. Khoảng cách giữa các bit nhúng được xác định bởi bộ tạo chuỗi giả ngẫu nhiên với sự phân bố đều giữa khoảng thời gian. Khó khăn chính của kỹ thuật giấu tin sử dụng luồng vật chứa chính là đồng bộ hóa, xác định sự bắt đầu và kết thúc chuỗi. Trong vật chứa, có thể chèn các bit đồng bộ hóa, tiêu đề gói tin vào trước các thông tin cần giấu. Giấu tin với luồng vật chứa không có tính khả thi cao do khó khăn trong việc tách tin.
- Vật chứa cố định: Trong một vật chứa cố định thì kích thước và đặc điểm của thông tin cần giấu cần cho biết trước. Vật chứa có thể được lựa chọn ngẫu nhiên hoặc lựa chọn trước. Vật chứa được chọn phụ thuộc vào thông tin mật cần giấu để không chỉ đảm bảo phải giấu được hết thông tin mà còn đảm bảo các yêu cầu đối với vật chứa sau khi giấu thông tin vào. Trong thực tế, hầu hết các ứng dụng thường lựa chọn giấu tin vào vật chứa được lựa chọn ngẫu nhiên. Các phương pháp giấu tin ngày nay thường sử dụng vật chứa cố định vì quá trình giấu tin và tách tin sẽ thuận lợi và dễ dàng hơn.

b) Phân loại theo môi trường giấu tin

Từ hình 1.2 có thể thấy các kỹ thuật giấu tin theo môi trường giấu tin được chia thành 4 hướng tiếp cận chính:

- *Giấu tin trong ảnh* là kỹ thuật giấu thông tin vào vật chứa là ảnh. Vật chứa có thể là ảnh tĩnh hoặc ảnh động. Hiện nay, giấu tin trong ảnh đang được ứng dụng và triển khai rộng rãi trong rất nhiều lĩnh vực như: xác thực thông tin, bảo vệ bản quyền tác giả, giấu thông tin mật... Chi tiết các phương pháp và kỹ thuật giấu tin trong ảnh được trình bày trong chương 2 của giáo trình.
- *Giấu tin trong âm thanh* là các phương pháp giấu thông tin vào vật chứa là các file âm thanh. Đặc điểm của phương pháp này là giấu thông tin vào trong các vùng âm thanh sao cho ngưỡng nghe của tai người không phát hiện ra những bất thường hoặc nhiễu do các thuật toán giấu tin gây ra. Các kỹ thuật giấu tin trong âm thanh cũng đang được quan tâm và sử dụng nhiều trong thực tế vì những lợi ích lớn của các phương pháp này mang lại. Trong chương 3, giáo trình sẽ trình bày một số phương pháp giấu tin trong âm thanh phổ biến hiện nay.

- *Giấu tin trong video* là các phương pháp nhằm giấu thông tin vào môi trường là các file video. Giấu tin trong video cũng được quan tâm và được phát triển mạnh mẽ cho nhiều ứng dụng như điều khiển truy nhập, xác thực thông tin và bảo vệ bản quyền tác giả, các hệ thống chương trình trả tiền xem theo video clip (pay per view application), ...
- *Giấu tin trong văn bản* là các phương pháp nhằm giấu thông tin vào môi trường là các tệp văn bản. Các tệp văn bản có thể là các file có định dạng như .docx, .pdf, .xlsx, giao thức mạng... Giấu tin trong văn bản khó thực hiện hơn do có ít các thông tin dư thừa.

Như vậy, có thể thấy rằng, đối với phương pháp giấu tin trong các môi trường giấu tin thì được chia thành 4 loại chính. Trong các nội dung của chương 2, chương 3 và chương 4 giáo trình sẽ phân tích chi tiết từng phương pháp và kỹ thuật giấu tin trong các môi trường ảnh, âm thanh và video. Do hạn chế về thời lượng, phần giấu tin trong văn bản không được trình bày trong giáo trình này. Độc giả quan tâm đến nội dung giấu tin trong văn bản có thể đọc thêm trong các tài liệu [1][32].

c) Phân loại theo cách thức tác động lên vật chứa tin

Có 3 phương pháp tác động lên vật chứa tin bao gồm:

- *Phương pháp chèn dữ liệu* là phương pháp tìm các vị trí trong tệp dễ bị bỏ qua và chèn thông tin cần giấu vào, cách giấu này không làm ảnh hưởng tới sự thể hiện các tệp dữ liệu.
- *Phương pháp thay thế* là phương pháp thay thế trực tiếp các giá trị của thông tin cần giấu vào các vị trí ít được chú ý và ít quan trọng nhất. Phương pháp này làm thay đổi vật chứa nhiều, xong nó có khả năng đánh lừa được các giác quan của con người (thị giác, thính giác). Phương pháp này có nhiều cách thực hiện như: thay thế trong miền không gian, tần số, thay thế các bit ít quan trọng, các kỹ thuật trải phổ, thống kê....
- *Phương pháp tạo các vật chứa*: Theo đó, từ các thông tin cần giấu sẽ tạo ra các vật chứa để phục vụ cho việc giấu tin đó. Người nhận dựa trên các vật chứa này sẽ tái tạo lại các thông điệp.

d) Phân loại theo mục đích sử dụng

Phân loại kỹ thuật giấu tin theo mục đích sử dụng có thể được phân theo 4 mục đích chính như sau:

- *Truyền thông tin mật*: Mục đích của phương pháp này là trao đổi thông tin mật đến một đối tượng khác mà không muốn đối tượng thứ ba có thể phát hiện ra hay nghi ngờ. Các kỹ thuật giấu theo hình thức này thường cố gắng giấu được càng nhiều thông tin vào vật chứa càng tốt nhưng vẫn đảm bảo chất lượng của vật chứa tin và tính vô hình của thông tin.
- *Chống chối bỏ bằng công nghệ nhúng số nhận dạng (hoặc dấu vân tay).* Công nghệ này có nhiều điểm chung với thủy vân số. Sự khác biệt là mỗi sản phẩm được bảo vệ sẽ được nhân bản ra thành nhiều bản sao hợp pháp. Mỗi bản sao có số nhận dạng của riêng nó được gọi là các "dấu vân tay". Mỗi số nhận dạng chỉ được gán cho một bản sao. Số nhận dạng này cho phép nhà sản xuất theo dõi các sản phẩm của mình. Khi một sản phẩm bị sao chép trái

phép, số nhận dạng này sẽ chỉ ra thủ phạm. Ví dụ: người mua A mua một bản sao hợp pháp của sản phẩm. Bản sao này có số nhận dạng riêng là X. Nếu như trên thị trường có nhiều bản sao có số nhận dạng X thì chứng tỏ người mua A đã sao chép trái phép sản phẩm này.

- *Nhúng tiêu đề:* Kỹ thuật nhúng tiêu đề được sử dụng để giấu các chữ ký vào vật chứa. Kỹ thuật này thường được sử dụng để lưu trữ thông tin không đồng nhất thành một bản duy nhất. Ví dụ trong y tế, các chuyên gia thường nhúng chữ ký bác sỹ, hình ảnh bệnh nhân, kết quả… vào hình ảnh y tế.
- *Thủy vân số* là phương pháp giấu thông tin (thủy vân) vào các vật chứa. Thủy vân là một thông tin nào đó mang ý nghĩa. Yêu cầu đối với thủy vân là một lượng thông tin rất nhỏ nhưng đủ mạnh để có thể bảo vệ vật chứa thủy vân. Ứng dụng của thủy vân số hiện nay rất đa dạng và hầu hết các lĩnh vực như: bảo vệ bản quyền hoặc chống xuyên tạc nội dung,…

e) Phân loại theo giao thức

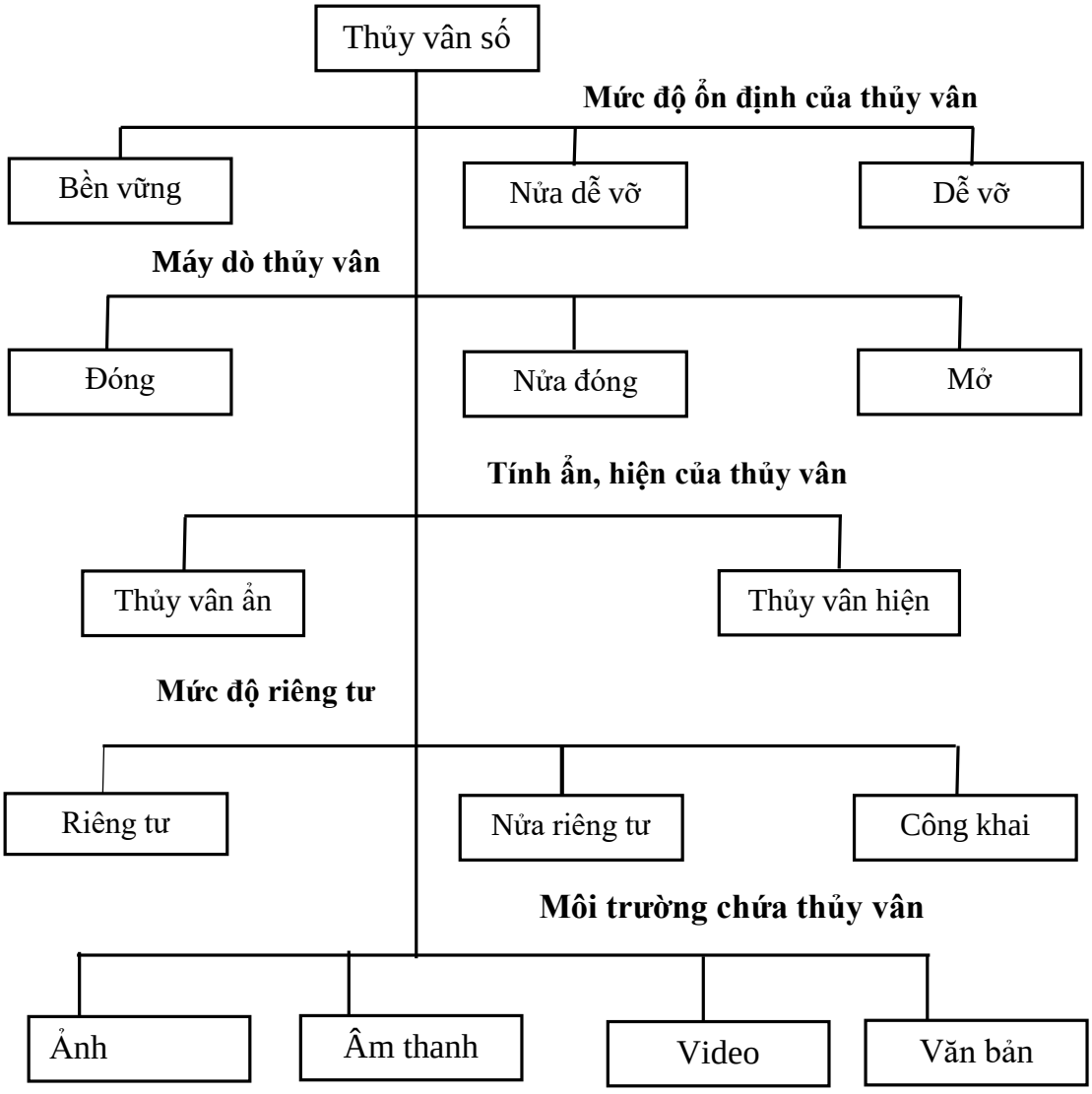
- *Giấu tin thuần túy:* là hệ thống giấu thông tin không yêu cầu phải trao đổi và thỏa thuận trước khi giấu. Người giấu tin và người tách tin cùng thực hiện một thuật toán giấu và tách thông tin. Thuật toán này cần phải giữ bí mật. Chính vì vậy mức độ bảo mật thông tin dựa trên chính thuật toán, vật chứa trước và sau khi giấu. Do đặc điểm của phương pháp giấu tin thuần túy nên trong quá trình giấu tin, người giấu tin thường sử dụng kỹ thuật mã hóa thông tin để mã hóa thông tin cần giấu trước khi mang đi giấu vào vật chứa.

- *Giấu tin sử dụng khóa bí mật:* là hình thức người gửi chọn vật chứa thông tin, sử dụng khóa bí mật, tiến hành giấu thông tin vào vật chứa đó. Khóa có thể được chọn bằng một số phương pháp như: dùng một số đặc tính của chính vật chứa làm khóa hoặc dùng hàm băm tính toán các giá trị này để làm khóa hoặc chọn các thành phần quan trọng trong vật chứa để làm khóa.
- *Giấu tin sử dụng khóa công khai*: Theo phương pháp này cần 2 khóa là khóa bí mật và khóa công khai. Khóa công khai được dùng trong quá trình giấu thông tin. Khóa bí mật chỉ có người nhận mới biết và dùng trong quá trình tách lấy thông tin, tái tạo lại thông tin ban đầu. Nguyên lý của giấu tin với khóa công khai là dùng thuật toán giải mã để giải mã trên mọi vật chứa thông tin mà không cần quan tâm việc vật chứa đó có chứa hay không chứa thông tin bí mật. Trong trường hợp vật chứa không có thông tin thì thông tin thu được khi giải mã chỉ là các phần tử ngẫu nhiên. Các phần tử ngẫu nhiên này gọi là các phần tử "ngẫu nhiên tự nhiên" của vật chứa.

1.2.2. Thủy vân số và phân loại thủy vân số

Trong các nội dung ở trên trên, giáo trình đã trình bày một số khái niệm, định nghĩa, lịch sử phát triển và vai trò của thủy vân số. Từ đây có thể thấy rằng thủy vân số là một trong những hướng tiếp cận tốt và được phát triển mạnh mẽ trong thời gian qua. Thực tế cho thấy, có nhiều ứng dụng của thủy vân số đã mang lại hiệu quả vượt trội so với các hướng tiếp cận khác như giấu tin mật hoặc mã hóa. Trong nội dung này, giáo trình sẽ trình bày một số hướng tiếp cận của thủy vân số đã và đang được nghiên cứu trong thời gian qua. Các nội dung này sẽ cung cấp cho người đọc cái nhìn tổng quát hơn về thủy vân số từ đó hiểu và biết cách áp

dụng chúng vào các ứng dụng thực tế. Hình 1.3 thể hiện các phương pháp chính trong lĩnh vực thủy vân số hiện nay.



Hình 1.3. Phân loại các phương pháp thủy vân số

Hình 1.3 liệt kê 4 hướng tiếp cận chính được phân loại theo thủy vân số. Theo đó, 4 phương pháp phân loại chính bao gồm:

a) Phân loại theo mức độ ổn định của thủy vân đối với các tác động

- Thủy vân số bền vững (Robust Watermarking): Là dạng thủy vân tồn tại bền vững trước các cuộc tấn công nhằm loại bỏ thủy vân. Trong trường hợp loại bỏ được thủy vân thì vật chứa tin cũng không còn giá trị sử dụng. Một ứng dụng điển hình của thủy vân bền vững chính là bảo vệ bản quyền: thuỷ vân được nhúng trong sản phẩm như một hình thức dán tem bản quyền.
- Thủy vân số nửa dễ vỡ (Semi Fragile Watermarking): Là dạng thủy vân tồn tại bền vững khi vật chứa tin bị sửa đổi vô hại như: nén, làm nhiễu, lọc,… nhưng lại nhạy cảm (dễ

vỡ) khi vật chứa tin bị sửa đổi độc hại như: đổi nội dung, cắt bỏ một phần. Thủy vân nửa dễ vỡ được thiết kế để phát hiện các sửa đổi độc hại trên sản phẩm (nhằm đảm bảo tính toàn vẹn của sản phẩm), đồng thời cho phép một số hoạt động sửa đổi vô hại trên sản phẩm.

- Thủy vân số dễ vỡ (Fragile Watermarking): Là dạng thủy vân nhạy cảm (dễ vỡ) trước mọi thay đổi của vật chứa tin, dù là thay đổi nhỏ nhất. Chính vì đặc điểm nhạy cảm như vậy nên thủy vân dễ vỡ được ứng dụng nhiều vào việc xác thực nội dung. Ví dụ: Khi một tòa soạn sử dụng một bức ảnh để đưa tin, toà soạn phải xác minh bức ảnh này đúng với ảnh gốc và chưa được chỉnh sửa.

b) Phân loại theo đầu vào của máy dò

Máy dò dùng để phát hiện vật chứa có chứa thủy vân hay không hoặc vị trí của thủy vân trong vật chứa. Tùy thuộc vào đầu vào của máy dò, hệ thống thủy vân được chia thành 3 loại chính là hệ thống đóng, hệ thống mở và hệ thống nửa đóng. Trong đó:

- *Hệ thống đóng*: đầu vào cần vật chứa gốc X, gồm 2 loại:
  + Loại 1: So sánh vật chứa có thủy vân S với vật chứa gốc X để tìm ra vị trí chứa thủy vân.
    - Đầu vào:
      - Vật chứa có thủy vân S.
      - Vật chứa gốc (vật chứa chưa có thủy vân) X.
      - Khóa K.
    - Đầu ra: Vị trí chứa thủy vân M.
  + Loại 2: So sánh vật chứa nghi ngờ có thủy vân S với vật chứa gốc X để tìm ra vị trí chứa thủy vân
    - Đầu vào:
      - Vật chứa có thủy vân S.
      - Vật chứa gốc (vật chứa chưa có thủy vân) X.
      - Khóa K.
      - Thủy vân M' là bản sao của thủy vân M.
    - Đầu ra: Trả lời có (1) hoặc không (0) cho câu hỏi: "Vật chứa tin S có chứa các thủy vân M không?".
- *Hệ thống nửa đóng*: Mục đích là để kiểm tra xem vật chứa S có chứa thủy vân M hay không?
  + Đầu vào:
    - Vật chứa tin S
    - Khóa K.
    - Thủy vân M' là bản sao của thủy vân M.
  + Đầu ra: Trả lời có (1) hoặc không (0) cho câu hỏi: "Vật chứa tin S có chứa các thủy vân M không?".
- *Hệ thống mở*: Mục đích là để kiểm tra xem vật chứa S có chứa thủy vân M hay không

+ Đầu vào:
    - Vật chứa tin *S*.
    - Khóa *K*.
+ Đầu ra: Thủy vân *M*.

c) Phân loại theo tính ẩn hay hiện

- Thủy vân hiện (Perceptible Watermarking): Là loại thuỷ vân được hiện ngay trên sản phẩm và mọi người dùng có thể nhìn thấy được. Với loại thủy vân hiện cần có biện pháp chống lại sự thay đổi hay loại bỏ thủy vân trái phép.
- Thủy vân ẩn (Imperceptible Watermarking): Khó có thể nhìn thấy thuỷ vân bằng mắt thường.

d) Phân loại theo mức độ riêng tư

- Thủy vân số riêng tư (private watermarking): chỉ có người dùng được ủy quyền có thể phát hiện ra thủy vân. Thủy vân riêng tư chống lại người dùng trái phép tìm cách tách thủy vân ra khỏi vật chứa thủy vân. Thủy vân số riêng tư được ứng dụng trong bảo vệ bản quyền (xem mục 1.4.2 xác thực nội dung).
- Thủy vân số nửa riêng tư (Semi private watermarking): cho phép mọi người đọc có thể phát hiện có thủy vân được giấu trong các vật chứa. Tuy nhiên người dùng không biết được thủy vân được giấu ở vị trí nào. Trong thủy vân nửa riêng tư mọi người đều biết quá trình phát hiện và đặc biệt là khoá phát hiện, do đó người giấu thủy vân cần sử dụng khóa bí mật để nhúng thủy vân và cung cấp khóa công khai lên mạng để mọi người xác minh thủy vân.
- Thủy vân số công khai (Public watermarking): cho phép mọi người đọc được thủy vân trong vật chứa tin nhưng không thể sửa, xóa thủy vân. Thủy vân số công khai được ứng dụng trong kiểm soát sao chép.

e) Phân loại theo môi trường chứa thủy vân

Từ hình 1.3 thấy được khi phân loại theo môi trường chứa thủy vân thì các kỹ thuật nhúng thủy vân sẽ được chia thành 4 loại chính bao gồm: ảnh, âm thanh, video, văn bản. Trong phần 1.2.1 đã mô tả chi tiết về khái niệm của 4 đối tượng này. Về cơ thì quá trình tiền xử lý các đối tượng này là tương đối giống nhau cho cả giấu tin mật và thủy vân số. Chúng chỉ khác nhau ở mục đích sử dụng của người dùng.

Dựa trên các định nghĩa và phân tích ở trên, có thể dễ dàng nhận thấy rằng các hướng tiếp cận và ứng dụng của thủy vân số rất phong phú và đa dạng. Bên cạnh đó, độc giả quan tâm có thể tìm hiểu sâu hơn về thủy vân số trong các tài liệu [2, 5].

1.3. Một số ứng dụng của kỹ thuật giấu tin

1.3.1. Lấy dấu vân tay (fingerprinting)

Lấy dấu vây tay là quá trình thêm dấu vân tay vào một đối tượng hoặc xác định dấu vân tay có sẵn của một đối tượng. Dấu vân tay là đặc điểm phân biệt một đối tượng này với

các đối tượng khác. Dấu vân tay của mỗi đối tượng là duy nhất. Các kỹ thuật lấy dấu vân tay không có tác dụng phòng chống giả mạo và do đó không ngăn người dùng sao chép dữ liệu trái phép. Kỹ thuật này chỉ cho phép chủ sở hữu tìm ra được người dùng đã phân phối chúng bất hợp pháp. Ví dụ: Trong truyền hình vệ tinh được mã hóa, người dùng có thể được cấp một bộ khóa để giải mã các luồng video. Đài truyền hình có thể chèn dấu vân tay vào từng gói dữ liệu để phát hiện các sử dụng trái phép. Nếu một người dùng cung cấp khóa giải mã của họ cho những người khác và những người này giải mã và xem video trái phép, thì đài truyền hình có thể truy tìm thủ phạm phát tán video trái phép. Để hiểu rõ hơn về ứng dụng của dấu vân tay, hãy cùng tìm hiểu ví dụ lấy dấu vân tay bất đối xứng trong mua bán hình ảnh số dưới đây [4]. Các chương trình lấy dấu vân tay đối xứng nghĩa là cả người mua và người bán đều biết bản sao này có dấu vân tay. Do đó, khi có bản sao được phân phối lại bất hợp pháp, thì có 2 nghi phạm trong trường hợp này: người mua ban đầu hoặc chính người bán. Điều đó dẫn đến việc người bán cố tình vu khống cho người mua hoặc người mua có thể dễ dàng chối bỏ hành vi sao chép của mình. Để giải quyết vấn đề, các chuyên gia sử dụng chương trình lấy dấu vân tay bất đối xứng, trong đó chỉ có người mua biết bản sao có dấu vân tay. Nếu sau đó người bán tìm thấy nó ở đâu đó, người bán có thể xác định người mua và chứng minh sự kiện này cho các bên thứ ba. Chương trình này bao gồm bốn giao thức: sinh khóa, nhúng dấu vân tay, xác định và tranh chấp [4].

1.3.2. Xác thực nội dung (content authentication)

Xác thực nội dung là quá trình kiểm tra và đánh giá nội dung của một đối tượng này với một đối tượng khác. Mục đích của xác thực nội dung là xác định các vi phạm đối với quy định. Để giải quyết được vấn đề này, các hướng tiếp cận truyền thống thường sử dụng kỹ thuật mã hóa bằng cách tạo một chữ ký số, chữ ký này sẽ được gắn liền với nội dung cần xác minh. Tuy nhiên chữ ký này dễ dàng bị mất đi trong quá trình truyền dữ liệu [5]. Ví dụ: Trường hợp chữ ký được gắn vào một hình ảnh dạng JPEG. Nếu hình ảnh này được chuyển đổi sang định dạng tệp khác, ảnh mới không có khoảng trống cho chữ ký trong tiêu đề, chữ ký sẽ bị mất và hình ảnh không còn được xác minh. Một giải pháp cho vấn đề này là nhúng trực tiếp chữ ký vào nội dung bằng kỹ thuật thủy vân số. Lúc này, chữ ký số sẽ được coi là một dấu hiệu xác thực. Dấu hiệu xác thực này được thiết kế sao cho khi nội dung bị sửa đổi (dù là sửa đổi nhỏ nhất), thì dấu hiệu này sẽ trở nên không hợp lệ (thủy vân dễ vỡ). Để thực hiện được nhiệm vụ tạo chữ ký và nhúng chữ ký này vào vật chứa có thể tiến hành tách nội dung làm hai phần: một phần để tính chữ ký, một phần để nhúng chữ ký. Ví dụ: tính toán một chữ ký từ các bit cao của hình ảnh và nhúng chữ ký vào trong các bit thấp của hình ảnh này. Một ý tưởng mở rộng hơn là thực hiện xác thực cục bộ. Theo đó, nếu một hình ảnh được chia thành các khối và mỗi khối có dấu hiệu xác thực riêng được nhúng trong nó. Người quản lý sẽ nhận biết những phần nào của hình ảnh đã được xác thực và những phần nào đã được sửa đổi. Ví dụ về một cuộc điều tra của cảnh sát về một tội phạm. Kịch bản là cảnh sát nhận được một video giám sát đã bị giả mạo. Nếu video được xác thực bằng chữ ký truyền

thống, cảnh sát sẽ biết là video đó không chính xác và không thể tin được. Tuy nhiên, nếu video này đã được xác thực cục bộ, họ có thể phát hiện ra rằng mỗi khung video đều đáng tin cậy ngoại trừ một số khung cảnh không được xác thực. Đây sẽ là bằng chứng mạnh mẽ cho thấy danh tính của một người có liên quan đến tội phạm đã bị xoá khỏi video.

1.3.3. Kiểm soát sao chép (copy control)

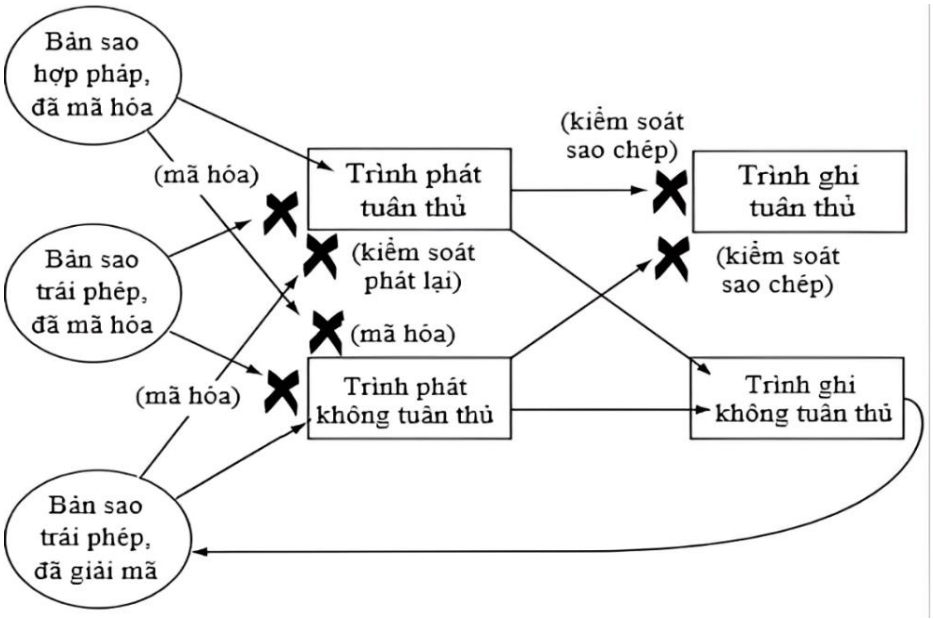
Kiểm soát sao chép là quá trình kiểm tra và giám sát để biết được thiết bị đó có quyền thế nào đến một đối tượng cụ thể. Trong thực tế, quyền đối với một đối tượng thường là các quyền đọc, ghi, phát... Như vậy, có thể thấy rằng, mục tiêu của kiểm soát sao chép là quá trình nhận dạng và trao quyền sao chép của thiết bị đến đối tượng. Để hỗ trợ kiểm soát sao chép, cách tiếp cận cơ bản nhất là nhúng thủy vân không bao giờ sao chép (never-copy watermark) vào dữ liệu và gắn sẵn các thiết bị phát hiện thuỷ vân vào trong các hệ thống đọc ghi. Mỗi khi có dữ liệu đi qua hệ thống đọc ghi, hệ thống này sẽ kiểm tra và đánh giá. Theo đó, phương pháp kiểm tra theo nguyên tắc sau [5]: Nếu dữ liệu không có thủy vân thì thiết bị đọc ghi cho phép sao chép dữ liệu. Nếu dữ liệu có thủy vân thì thiết bị đọc ghi cấm sao chép dữ liệu. Tuy nhiên cách tiếp cận này có hạn chế là không phải tất cả hệ thống đọc ghi đều có gắn thiết bị phát hiện thủy vân do nhà sản xuất phải mất thêm chi phí lắp đặt và khách hàng thì thích thiết bị có khả năng tạo bản sao trái phép. Để chống lại điều này, có thể sử dụng một ý tưởng được gọi là kiểm soát phát lại. Để hiểu rõ hơn về vấn đề này hãy xét đến hệ thống chống sao chép đĩa DVD có các định nghĩa sau:

- Trình phát tuân thủ: là trình phát chỉ phát bản sao hợp pháp.
- Trình ghi tuân thủ: là trình ghi không cho phép sao chép bản sao có thủy vân chống sao chép (never-copy).
- Trình phát không tuân thủ: là trình phát cho phép phát mọi loại bản sao.
- Trình ghi không tuân thủ: là trình ghi cho phép sao chép mọi loại bản sao.

Ý tưởng kiểm soát phát được mô tả như hình 1.4.

Kịch bản của kiểm soát sao chép bằng kỹ thuật giấu tin như sau trên hình 1.4 như sau: Một người dùng mua đĩa DVD từ cửa hàng. Người dùng không biết đĩa DVD này là bản sao hợp pháp hay bất hợp pháp. Lúc này sẽ có những trường hợp như sau:

- Nếu đĩa DVD là một bản sao hợp pháp đã được mã hóa thì sẽ có khả năng:
  + Có thể phát trên một trình phát tuân thủ do có khóa để giải mã bản sao này.
  + Không thể phát trên một trình phát không tuân thủ do trình phát này không có khóa để giải mã bản sao này.
  + Đầu ra của trình phát tuân thủ:
    - Không thể được sao chép bởi trình ghi tuân thủ do trình ghi này cấm sao chép bản sao có chứa thủy vân không sao chép.
    - Có thể được sao chép bởi trình ghi không tuân thủ, kết quả thu được bản sao trái phép đã được giải mã (do đầu vào là bản sao hợp pháp đã được giải mã).



Hình 1.4. Ứng dụng giấu tin trong kiểm soát sao chép

- Nếu đĩa DVD là một bản sao trái phép đã được giải mã sẽ có một số trường hợp sau:

+ Không thể phát trên một trình phát tuân thủ do trình phát này phát hiện thủy vân và sau khi kiểm tra phát hiện thủy vân này không hợp lệ.

+ Có thể phát trên trình phát không tuân thủ do bản sao này không bị mã hóa.

+ Đầu ra của trình phát không tuân thủ:

o Không thể được sao chép bởi trình ghi tuân thủ do phát hiện thủy vân trên bản sao trái phép.

o Có thể được sao chép bởi trình ghi không tuân thủ.

- Nếu đĩa DVD bản sao trái phép đã mã hóa (bản sao chép đơn thuần chưa được giải mã) sẽ không thể phát trên mọi trình phát do:

+ Không thể phát trên một trình phát tuân thủ do trình phát này phát hiện thủy vân và sau khi kiểm tra phát hiện thủy vân này không hợp lệ.

+ Không thể phát trên một trình phát không tuân thủ do trình phát này không có khóa để giải mã bản sao này.

Từ đây, khách hàng có hai lựa chọn: Mua một thiết bị tuân thủ, chỉ có thể phát nội dung hợp pháp, không thể phát nội dung vi phạm bản quyền (luôn phải mua nội dung hợp pháp) hoặc mua một thiết bị không tuân thủ, có thể phát nội dung vi phạm nhưng không thể phát nội dung hợp pháp (luôn phải dùng hàng lậu). Ví dụ với một bộ phim hay chỉ có DVD hợp pháp mà không có DVD sao chép trái phép thì khách hàng này dù có bỏ tiền ra mua DVD hợp pháp cũng không thể xem được bộ phim này.

1.3.4. Bảo vệ bản quyền tác giả (Copyright protection)

Ứng dụng của giấu tin trong vấn đề bảo vệ bản quyền tác giả là một trong những ứng dụng phổ biến hiện nay. Các kỹ thuật thủy vân số đã được nghiên cứu và áp dụng để giải

quyết nhiệm vụ này. Theo đó, một thông tin nào đó mang ý nghĩa quyền sở hữu tác giả sẽ được nhúng vào trong các sản phẩm. Thủy vân đó chỉ một mình người chủ sở hữu hợp pháp các sản phẩm đó có và được dùng làm minh chứng cho bản quyền sản phẩm [2, 5]. Giả sử có một sản phẩm dữ liệu số như ảnh, âm thanh, video được lưu thông trên mạng. Để bảo vệ các sản phẩm chống lại hành vi lấy cắp hoặc làm giả cần phải có một kỹ thuật để "dán tem bản quyền" vào sản phẩm này. Việc dán tem hay 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 đó. Muốn bỏ thuỷ vân này mà không được phép của người chủ sở hữu thì chỉ còn cách là phá huỷ sản phẩm đó.

1.3.5. Một số ứng dụng khác

Ngoài những ứng dụng phổ biến như trình bày trong mục 1.3.4 ở trên, các kỹ thuật giấu tin cũng còn được ứng dụng vào một số lĩnh vực khác như truyền thông tin mật. Đây là ứng dụng để liên lạc bí mật giữa hai bên tham gia truyền thông mà không bị bên thứ ba phát hiện [2, 3, 5]. Bên cạnh đó, các kỹ thuật giấu tin cũng được những kẻ tấn công, những kẻ xấu sử dụng để phát tán mã độc hoặc tấn công mạng. Cụ thể, những kẻ tấn công sử dụng các kỹ thuật giấu tin để giấu mã độc vào các môi trường đa phương tiện rồi phát tán chúng đến nạn nhân. Khi nạn nhân mở các file đa phương tiện này thì mã độc sẽ được kích hoạt và gây ảnh hưởng đến hệ thống. Ví dụ: Vào năm 2015, phần mềm độc hại của Vawtrak/ Neverquest bắt đầu sử dụng giấu tin để ẩn các cài đặt trong favicons. Phần mềm độc hại này sử dụng các bit quan trọng nhất từ mỗi điểm ảnh của hình ảnh để tái tạo lại một URL được nhúng trước đó để tải tập tin cấu hình của nó. Ngoài ra, các phần mềm độc hại như Ramsomware giấu tệp tin thực thi mã hóa trong các hình ảnh. Khi người dùng tải hình ảnh về, tệp tin độc hại này được thực thi, kết quả là toàn bộ dữ liệu trong máy người dùng bị mã hóa. Một ví dụ khác là Stegobot. Stegobot là mạng máy tính mà các máy trong mạng bị nhiễm mã độc thông qua giấu tin mật. Kẻ tấn công có thể điều khiển các máy trong mạng này từ xa và thực hiện những hành động mà chủ sở hữu của các máy này không hề hay biết. Một mạng Stegobot có thể có tới hàng trăm nghìn, thậm chí là hàng triệu máy tính.

1.4. Giới thiệu về tấn công lên các kỹ thuật giấu tin

Thực tế cho thấy, các kỹ thuật giấu tin từ lúc ra đời và được ứng dụng trong thực tế rộng rãi như ngày nay luôn mang trong mình quá trình đấu tranh để phát triển. Các thuật toán, phương pháp giấu tin sẽ bị thay thế bởi các phương pháp mới nếu chúng được chứng minh không còn an toàn và hiệu quả. *Tấn công lên các phương pháp giấu tin (Steganalysis)* là ngành khoa học chuyên nghiên cứu, áp dụng các phương pháp, kỹ thuật, thuật toán nhằm phát hiện dữ liệu ẩn và trích xuất hoặc phá hủy nó. Một cuộc tấn công được xem là thành công hay không tuỳ theo ứng dụng. Ví dụ, đối với liên lạc bí mật, việc phát hiện và chứng minh được vật chứa có chứa tin mật được coi là thành công. Đối với bảo vệ bản quyền hay chống giả mạo thì việc tấn công được coi là thành công nếu không chỉ phát hiện mà còn làm hư hại hoặc phá hủy thủy vân trong khi vẫn bảo toàn chất lượng của vật chứa.

Các kỹ thuật tấn công lên giấu tin có thể được chia thành hai loại chính là tấn công cố ý và tấn công vô ý. Trong đó, tấn công cố ý là người tấn công cố tình, chủ động thực hiện các biện pháp, kỹ thuật nhằm tác động gây ảnh hưởng đến vật chứa. Mục đích duy nhất của tấn công cố ý là cố gắng loại bỏ thủy vân. Tấn công vô ý là các hành vi không cố ý làm ảnh hưởng đến vật chứa. Tấn công vô ý xảy ra trong suốt quá trình xử lý vật chứa thông thường ví dụ như nén có tổn hao, nhiễu trên đường truyền và một vài thao tác khác như cắt, lọc,... Các tác động này có thể gây khó khăn trong quá trình trích rút thủy vân.

Trong thực tế có thể chia các kỹ thuật tấn công lên giấu tin làm bốn loại như sau: Tấn công loại bỏ, tấn công hình học, tấn công mật mã và tấn công giao thức. Trong đó:

- Tấn công loại bỏ (Removal attack) là dạng tấn công chú trọng vào việc loại bỏ hoàn toàn thông tin thủy vân từ dữ liệu nhúng thủy vân mà không ảnh hưởng hay gây ra những tác động có thể nhận biết đến tính an toàn của dữ liệu. Có nghĩa là không có giải thuật nào có thể khôi phục lại thông tin thủy vân từ dữ liệu nhúng. Loại tấn công này gồm có các quá trình triệt nhiễu, lượng tử, nén có tổn hao, tái điều chế....

- Tấn công hình học (Geometrical attacks): Ngược với tấn công loại bỏ, dạng tấn công này không chú trọng loại bỏ thông tin được nhúng mà cố gắng tìm cách làm sai lệch thông tin này bằng cách thay đổi về thời gian hoặc không gian của dữ liệu đã nhúng thủy vân. Một trong các hướng tiếp cận chủ yếu được thực hiện trong kỹ thuật tấn công này là tấn công vào sự đồng bộ giữa thiết bị phát hiện dữ liệu và thông tin giấu. Bởi vì khi sự đồng bộ này bị ảnh hưởng thì thiết bị phát hiện sẽ không thể phát hiện ra vị trí giấu tin. Điều này sẽ gây ảnh hưởng rất lớn đến quá trình tách tin. Ví dụ, đối với ảnh nhúng thủy vân, những kẻ tấn công sẽ tìm cách xáo trộn các điểm ảnh dẫn đến người giấu tin không thể tách được thông tin.

- Tấn công mật mã (Cryptographic attack): Dạng tấn công này sẽ bẻ gãy tính an toàn của hệ thống thủy vân và tìm cách loại bỏ thông tin thủy vân hoặc nhúng thủy vân giả. Một dạng tấn công thuộc dạng này được biết đến là Oracle, nó tạo ra ảnh không có thủy vân khi một bộ phát hiện thủy vân được sử dụng.

- Tấn công giao thức (Protocol attack). Có 2 loại tấn công giao thức: tấn công đảo ngược (inverse attack) và tấn công sao chép (copy attack). Dạng tấn công đảo ngược dựa trên cơ chế thủy vân có thể đảo ngược, kẻ tấn công có thể tuyên bố là chủ sở hữu của dữ liệu, vì dữ liệu cũng chứa thủy vân của kẻ tấn công nên khi trích ra thủy vân thì sẽ ra thủy vân của chính kẻ tấn công. Việc này tạo ra sự không rõ ràng trong việc xác định người chủ bản quyền. Còn tấn công sao chép là dạng tấn công không tìm cách phá hủy hay làm hư hại việc phát hiện thủy vân. Kỹ thuật tấn công này sẽ thực hiện sao chép thủy vân cho những vật chứa khác. Dạng tấn công sao chép không cần biết giải thuật thủy vân số cũng như khóa sử dụng trong quá trình nhúng thủy vân. Trong thực tế, một kẻ tấn công cố ý thường không chỉ dùng một loại mà kết hợp nhiều loại tấn công cùng một lúc để đạt được mục tiêu của mình.

1.5. Tổng kết chương 1

Trong chương một, giáo trình đã trình bày các kiến thức tổng quát về lĩnh vực giấu tin. Cụ thể:

- Trình bày một số định nghĩa, khái niệm và các thành phần cơ bản cũng như các yêu cầu tối thiểu đối với kỹ thuật giấu tin.

- Liệt kê và phân tích một số phương pháp và tiêu chí phân loại các kỹ thuật giấu tin. Dựa trên sự phân loại có hệ thống này, giáo trình không chỉ đưa ra cái nhìn tổng quát về các phương pháp giấu tin mà còn cung cấp cơ sở để lựa chọn các thuật toán, phương pháp giấu tin cho từng ứng dụng thực tế.

- Mô tả một số ứng dụng cơ bản của kỹ thuật giấu tin. Theo đó, trong chương một, giáo trình đã đi sâu vào bốn ứng dụng chính của các kỹ thuật giấu tin bao gồm: kiểm soát sao chép, bảo vệ bản quyền tác giả, lấy dấu vân tay và xác thực nội dung.

- Giới thiệu về một số phương pháp tấn công lên các kỹ thuật giấu tin. Dựa trên các phân tích và đánh giá trong chương một, có thể nhận ra rằng các phương pháp tấn công lên kỹ thuật giấu tin sẽ sử dụng hai hướng tiếp cận chính là tấn công trực tiếp vào vật chứa và tấn công vào thông tin giấu.

1.6. Câu hỏi ôn tập và thực hành

Câu 1. Liệt kê và phân tích về các yêu cầu đối với kỹ thuật giấu tin?

Câu 2. Hãy vẽ sơ đồ tổng quát của mô hình giấu tin và tách tin? Hãy giải thích các tham số trong mô hình giấu tin và tách tin?

Câu 3. Phân tích vai trò của giấu tin trong ứng dụng bảo vệ bản quyền tác giả?

Câu 4. Phân tích vai trò của giấu tin trong ứng dụng kiểm soát sao chép?

Câu 5. Phân tích vai trò của giấu tin trong ứng dụng xác thực nội dung?

Câu 6. Phân tích vai trò của giấu tin trong ứng dụng lấy dấu vân tay?

Câu 7. Trình bày khái niệm về thủy vân bền vững? Hãy lấy ví dụ minh họa của thủy vân bền vững?

Câu 8. Thủy vân dễ vỡ là gì? Hãy lấy ví dụ minh họa của thủy vân dễ vỡ.

Câu 9. Hãy nêu định nghĩa về thủy vân riêng tư? Lấy ví dụ minh họa của thủy vân riêng tư?

Câu 10. Hãy định nghĩa về giấu tin mật và thủy vân số? Phân tích vai trò và tầm quan trọng của kỹ thuật giấu tin trong an toàn thông tin.

Câu 11. Hãy nêu định nghĩa về phương pháp tấn công lên các kỹ thuật giấu tin? Hãy lấy ví dụ minh họa.

Câu 12. Liệt kê và phân tích đặc điểm của các phương pháp tấn công lên các kỹ thuật giấu tin.

Câu 13. Lấy 1 video, hãy thực hiện trích xuất hoặc thêm dấu vân tay (tùy ý) vào video trên bằng công cụ Vidupe.

Câu 14. Cài đặt và cấu hình công cụ xACRCloud để thực hiện xác thực thông tin.

Câu 15. Cài đặt và cấu hình công cụ DVD Copy Protect để kiểm soát sao chép.

Câu 16. Hãy tìm hiểu về cơ chế thu và phát trực tuyến của giải bóng đá ngoại hạng Anh? Dựa vào các phương pháp giấu tin đã biết, hãy giải thích vì sao ban tổ chức các giải đấu này có khả năng phát hiện được đài truyền hình nào đang vi phạm bản quyền truyền hình?

Câu 17. Cài đặt công cụ VSCode và thử nghiệm tấn công hình học lên ảnh.

CHƯƠNG 2: GIẤU TIN TRONG ẢNH

2.1. Một số vấn đề của giấu tin trong ảnh

2.1.1. Khái niệm về giấu trong ảnh

Như đã trình bày trong phần phân loại giấu tin trong môi trường đa phương tiện, giấu tin trong ảnh là kỹ thuật giấu tin mà trong đó thông tin sẽ được giấu trong dữ liệu ảnh. Các kỹ thuật giấu tin trong ảnh được thực hiện sao cho chất lượng ảnh ít bị thay đổi nhất để bằng mắt thường con người không thể phát hiện ra sự thay đổi đó. Cụ thể, các thuật toán giấu tin sẽ tìm cách khai thác và lợi dụng sự hạn chế về cảm nhận hình ảnh của con người để giấu thông tin. Tùy theo từng ứng dụng mà các kỹ thuật giấu tin có những tính chất và yêu cầu khác nhau. Nhưng tựu chung lại, các kỹ thuật giấu tin trong ảnh không chỉ phải đảm bảo tất cả các tính chất của kỹ thuật giấu tin yêu cầu mà còn phải đảm bảo một số tính chất riêng đối với môi trường ảnh [1, 2, 3]. Ngày nay, kỹ thuật giấu tin trong ảnh thường được sử dụng để truyền thông tin mật giữa người dùng mà người khác không thể biết được. Chính từ những lợi ích mà các kỹ thuật giấu tin trong ảnh mang lại nên hiện nay lĩnh vực giấu tin trong ảnh đang được phát triển nhanh chóng và mạnh mẽ. Ví dụ như đối với các nước phát triển, chữ kí tay đã được số hóa và lưu trữ sử dụng như là hồ sơ cá nhân của các dịch vụ ngân hàng và tài chính, nó được dùng để xác thực trong các thẻ tín dụng của người tiêu dùng. Ngoài ra phần mềm Microsoft Word cũng cho phép người dùng lưu trữ chữ kí trong ảnh nhị phân rồi gắn vào vị trí nào đó trong file văn bản để đảm bảo tính toàn vẹn của thông tin.

2.1.2. Một số định dạng ảnh và công cụ xử lý ảnh

a) Một số định dạng ảnh

Hiện nay có nhiều loại định dạng ảnh khác nhau có thể được lựa chọn để giấu tin. Mỗi định dạng ảnh sẽ có tiêu chuẩn và tính chất khác nhau. Do đó, để tối ưu hóa quá trình giấu tin thì trước khi tiến hành giấu tin người giấu tin cần phải xem xét và đánh giá các định dạng, tiêu chuẩn ảnh. Tiếp theo, giáo trình sẽ cung cấp một số mô tả về một số định dạng ảnh đang được sử dụng phổ biến hiện nay.

- **Định dạng ảnh BMP [6]:** BMP được biết đến với tên tiếng Anh khác là Windows bitmap, là một định dạng ảnh phổ biến. Định dạng ảnh BMP được sử dụng để lưu trữ hình ảnh kỹ thuật số bitmap, độc lập với thiết bị hiển thị và có khả năng lưu trữ hình ảnh kỹ thuật số hai chiều cả đơn màu, đa màu, ở các độ sâu màu khác nhau tùy vào dữ liệu nén, các kênh alpha và các cấu hình màu. Một tập tin Bitmap bao gồm các cấu trúc theo thứ tự như biểu trên Bảng 2.1.

Bảng 2.1. Cấu trúc tập tin Bitmap

Tên cấu trúc	Kích thước	Mục đích
Tiêu đề tệp Bitmap	14 byte	Lưu trữ thông tin tổng quát về tệp hình ảnh bitmap
Tiêu đề DIB	Tùy theo các phiên bản	Lưu trữ thông tin chi tiết về ảnh bitmap và xác định định dạng điểm ảnh
Mặt nạ thêm bit	12 hoặc 16 byte	Xác định định dạng điểm ảnh.
Bảng màu	Tùy theo các phiên bản	Xác định màu sắc được sử dụng bởi dữ liệu hình ảnh bitmap
Gap1	Tùy theo các phiên bản	Cân chỉnh cấu trúc
Mảng điểm ảnh	Tùy theo các phiên bản	Xác định giá trị các điểm ảnh
Gap2	Tùy theo các phiên bản	Cân chỉnh cấu trúc
Màu ICC	Tùy theo các phiên bản	Xác định cấu hình màu để quản lý màu sắc

Từ bảng 2.1 có thể thấy được định dạng BMP có cấu trúc tương đối đơn giản. Ngoài ra, khi ảnh BMP không nén thì các ảnh này chỉ là một ma trận các điểm ảnh. Trong đó, mỗi một phần tử của ma trận biểu diễn một điểm ảnh, bao gồm các thành phần đỏ (kí hiệu R), xanh lục (kí hiệu G), xanh lam (kí hiệu B), alpha (kí hiệu A), các thành phần bổ sung (kí hiệu X). Ngày này các kỹ thuật giấu tin trong ảnh sử dụng ảnh theo chuẩn BMP không được sử dụng phổ biến. Bởi vì các ảnh này có cấu trúc đơn giản, do đó giấu được ít thông tin cũng như thông tin sau khi giấu dễ bị phát hiện.

- Định dạng ảnh PNG: PNG (Portable Network Graphics) là một dạng ảnh sử dụng phương pháp nén dữ liệu không làm mất đi dữ liệu gốc. PNG hỗ trợ các ảnh dựa trên bảng màu (với bảng màu RGB 24 bit hoặc RGBA 32 bit), ảnh xám (có hoặc không có kênh alpha) và ảnh RGB/RGBA không có bảng màu đầy đủ. Các giá trị trong phần tiêu đề của định dạng ảnh PNG được liệt kê trong bảng 2.2.

Bảng 2.2. Các giá trị trong tiêu đề tập tin PNG

Giá trị	Mục đích
89	Có các bit cao thiết lập để phát hiện các hệ thống truyền dẫn không hỗ trợ dữ liệu 8 bit, giảm nguy cơ mà một tập tin văn bản bị hiểu nhầm là một tập PNG, hoặc ngược lại.
50 4E 47	Là chữ cái PNG trong bảng mã ASCII, cho phép xác định định dạng PNG
0D 0A	Là một kiểu kết thúc của DOS giúp phát hiện dòng kết thúc chuyển đổi dữ liệu
1A	Một byte thông báo dừng hiển thị của tập tin

Ngoài các thành phần tiêu đề tập tin PNG được mô tả trong bảng 2.2 thì chuẩn PNG còn có các đoạn mã lưu trữ dữ liệu (chunk). Đoạn mã lưu trữ dữ liệu này là một đoạn thông tin được sử dụng trong nhiều định dạng đa phương tiện. Mỗi một đoạn mã lưu trữ dữ liệu truyền tải thông tin nhất định về hình ảnh. Có hai loại đoạn mã lưu trữ dữ liệu: một là đoạn mã chính, hai là đoạn mã phụ trợ. Một bộ giải mã có khả năng đọc các đoạn mã lưu trữ dữ liệu quan trọng và hiển thị tệp PNG. Các đoạn mã lưu trữ dữ liệu phụ trợ là các thuộc tính hình ảnh khác có thể được lưu trữ trong các tệp PNG bao gồm các giá trị gamma, màu nền… Các đoạn mã lưu trữ dữ liệu quan trọng bao gồm IHDR, PLTE, IDAT, IEND. Giá trị của các IHDR, PLTE, IDAT, IEND được mô tả trong tài liệu [7].

- Định dạng ảnh JPEG: JPEG (Joint Photographic Experts Group) một nhóm các nhà nghiên cứu đã phát minh ra định dạng này để hiển thị các hình ảnh đầy đủ màu hơn mà kích thước file lại nhỏ hơn. Chuẩn JPEG có thể hiển thị các hình ảnh với các màu chính xác lên đến 16 triệu màu. Cấu trúc ảnh JPEG bao gồm nhiều phân đoạn (segment), ở mỗi đoạn là 1 cờ (marker), mỗi cờ bắt đầu bằng byte 0xFF và theo sau đó là 1 byte chỉ ra mã của loại cờ. Một số cờ chỉ gồm 2 byte; sau 2 byte cờ là 2 byte chỉ ra độ dài của đoạn không tính 2 byte của cờ. Với những đoạn chứa dữ liệu nén (entropy-coded data), 2 byte xác định độ dài của đoạn không tính độ dài của dữ liệu nén. Ảnh JPEG không yêu cầu các đoạn phải nằm theo đúng thứ tự nhưng đoạn đầu tiên của ảnh phải là đoạn SOI; đoạn cuối cùng là đoạn EOI. Một số thuộc tính của những cờ thường gặp trong ảnh JPEG được mô tả trong bảng 2.3 [8].

Bảng 2.3. Mô tả một số cờ thông dụng trong ảnh JPEG [9]

Tên rút gọn	Giá trị cờ	Mô tả tóm tắt
SOI	0xFF, 0xD8	Đánh dấu bắt đầu ảnh JPEG
SOFn	0xFF, 0xCn	Bắt đầu của khung, mô tả các thông số của ảnh: chiều cao, chiều rộng, số lượng thành phần màu, tỉ lệ số lượng thành phần màu.
DHT	0xFF, 0xC4	Xác định bảng Huffman. Trong ảnh JPEG có thể xuất hiện nhiều đoạn DHT
DQT	0xFF, 0xDB	Xác định bảng lượng tử hóa. Trong ảnh JPEG có thể xuất hiện nhiều đoạn DQT
SOS	0xFF, 0xDA	Đánh dấu bắt đầu quét ảnh từ trên xuống dưới.
APPn	0xFF, 0xEn	Dành riêng cho đoạn ứng dụng, đánh dấu bắt đầu của đoạn dữ liệu ứng dụng.
COM	0xFF, 0xEE	Cờ bắt đầu chứa lời bình (chú thích).
EOI	0xFF, 0xD9	Đánh dấu kết thúc ảnh

Từ bảng 2.3 có thể thấy được ảnh JPEG có cấu trúc phức tạp bao gồm nhiều thành phần khác nhau. Dựa trên đặc điểm của các thành phần này, các phương pháp giấu tin trong ảnh sẽ khai thác để thực hiện giấu tin.

b) Một số công cụ xử lý ảnh phổ biến

Các công cụ xử lý ảnh hiện nay đóng vai trò quan trọng trong việc triển khai các phương pháp giấu tin trong ảnh và xử lý ảnh chuyên sâu. Sau đây là một số công cụ thường để xử lý ảnh phổ biến: Corel PaintShop Pro, GIMP, Adobe Photoshop Elements, Paint.NET, Photo Pos Pro, Zoner Photo Studio, PhotoScape, Xara Photo & Graphic Designer.

2.1.3. Phân loại kỹ thuật giấu tin trong ảnh

Các phương pháp, thuật toán giấu tin trong ảnh đang được chia thành 3 loại chính bao gồm [1, 2, 5, 10, 14]:

- Giấu tin trên miền không gian ảnh: là kỹ thuật giấu tin mà các thông tin được giấu trực tiếp vào các điểm ảnh. Một số thuật toán và kỹ thuật thường được sủ dụng để giấu tin trong miền không gian như [10, 14]: LSB (Least Significant Bit); Hoán vị giả ngẫu nhiên (Pseudo-random Permutation); Phương pháp giấu khối; Phương pháp Brundox; Phương pháp Darmstadter-Dellegle-Quisquotter-McCa. Đặc điểm của các kỹ thuật giấu tin trong miền không gian là ảnh chứa tin sẽ không hoặc ít khi bị xử lý trước khi thực hiện giấu tin. Do đó, các kỹ thuật giấu tin trên miền không gian thường có hiệu quả thấp theo cả 2 tiêu chí: số lượng tin giấu và chất lượng hình ảnh sau khi giấu.

- Giấu tin trong miền tần số ảnh: Đây là kỹ thuật giấu tin mà trong đó các dữ liệu về điểm ảnh sẽ được biến đổi độc lập sang các dạng dữ liệu khác. Sau đó, thông tin sẽ được giấu vào các dữ liệu mới này. Như vậy, khác với kỹ thuật giấu tin trong miền không gian, các kỹ thuật giấu tin trong miền tần số thường tiến hành xử lý ảnh chứa tin rồi mới tiến hành giấu thông tin. Một số thuật toán và kỹ thuật thường được dụng để xử lý ảnh và giấu tin trong miền tần số ảnh như: Biến đổi cosine rời rạc (DCT - Discrete Cosine Transformations); Biến đổi Wavelet rời rạc (DWT - Discrete Wavelet Transform); Biến đổi Fourier rời rạc (DFT - Discrete Fourier Transform); Phương pháp Koch và Zhao; Phương pháp Bengam- Memon-Eo-Young; Phương pháp Hsu and Wu,... Các phương pháp giấu tin trong ảnh theo miền tần số mang lại hiệu quả tốt và giấu được nhiều thông tin và đảm bảo được tính bí mật. Hiện nay hầu hết các ứng dụng đều sử dụng kỹ thuật giấu tin trên miền tần số.

2.2. Phương pháp giấu tin trong miền không gian

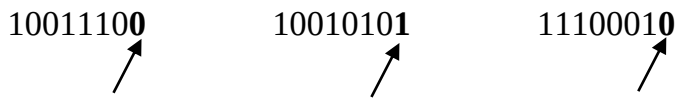
2.2.1. Phương pháp thay thế

a) Tổng quan về phương pháp thay thế LSB

LSB là bit có trọng số thấp nhất trong mỗi điểm ảnh [10]. Vì là bit có trọng số thấp nhất trong các điểm ảnh nên việc khi thay đổi giá trị các bit đó sẽ không ảnh hưởng nhiều đến chất lượng hình ảnh gốc. Việc xác định LSB của mỗi điểm ảnh trong một bức ảnh phụ thuộc vào định dạng của ảnh và số bit màu dành cho mỗi điểm của ảnh đó. Ví dụ đối với ảnh 16 bit thì 15 bit là biểu diễn 3 màu RGB của điểm ảnh còn bit cuối cùng không dùng đến thì ra sẽ tách bit này ra ở mỗi điểm ảnh để giấu tin, hoặc với ảnh 256 màu thì bit cuối cùng trong 8 bit biểu diễn một điểm ảnh được coi là bit ít quan trọng nhất,… Lợi dụng tính chất này mà

những người giấu tin sẽ tìm cách thay thế các LSB bằng các bit của thông tin cần giấu. Để hiểu rõ hơn về vấn đề này, hãy xem ví dụ được trình bày trong hình 2.1.

Ví dụ: Tách bit cuối cùng trong 8 bit biểu diễn mỗi điểm ảnh của ảnh 256



Hình 2.1. Bit có trọng số thấp LSB

Theo hình 2.1 coi bit cuối cùng là bit ít quan trọng nhất, thay đổi giá trị của bit này sẽ thay đổi giá trị của điểm ảnh lên hoặc xuống đúng một đơn vị, ví dụ như giá trị điểm ảnh là 234 thì khi thay đổi bit cuối cùng nó có thể mang giá trị mới là 235 nếu đổi bit cuối cùng từ 0 thành 1. Với sự thay đổi nhỏ đó thì cấp độ màu của điểm ảnh sẽ không bị thay đổi nhiều.

b) Quy trình giấu tin và tách tin trên k bit LSB

- *Phương pháp giấu tin*

+ Đầu vào của phương pháp bao gồm:
  - Ảnh gốc *C*.
  - Thông điệp bí mật *M*.
+ Đầu ra: Ảnh mang tin.

Các bước cơ bản trong quá trình giấu tin vào trong ảnh sử dụng *k* bit LSB như sau:

Bước 1: Với *C* là ảnh nguyên bản 8-bit màu xám, kích thước $M_c \times N_c$ điểm ảnh. Người giấu tin sẽ thực hiện biểu diễn ma trận điểm ảnh về dạng số thập phân. Công thức biến đổi tổng quát như sau: $C = \{x_{ij} | \ 0 \le i \le M_c, 0 \le j \le N_c, x_{ij} = \{0, 1, 2, \ldots, 255\}\}$. Sau khi ảnh *C* đã được chuyển thành ma trận điểm ảnh thì tiếp tục chuyển ma trận điểm ảnh này về mảng 1 chiều *I* với *i* phần tử, sau đó chuyển các điểm ảnh về dạng nhị phân.

Bước 2*:* thông điệp *M* chiều dài *n* bit sẽ chuyển về dạng nhị phân theo công thức (2.1):

$$M = \{m_i | \ 0 \le i < n, m_i \{0,1\}\} \quad (2.1)$$

Bước 3: Thực hiện giấu tin. Cứ 8 bit ảnh tách bỏ số bit LSB ngoài cùng bên phải và ghép phần còn lại với *k* bit nhị phân đầu của thông điệp (*k* có thể là 2 hoặc 4 bit), kết quả thu được đưa về dạng thập phân rồi gán ngược lại vào *I*(i). Cuối cùng chuyển đổi ảnh giá trị nhị phân trong mảng *I* từ mảng một chiều về mảng 2 chiều $M_c \times N_c$ phần tử. Ảnh mới thu được là ảnh đã chứa tin giấu.

- *Phương pháp tách tin*

Cũng tương tự như quá trình giấu tin trong ảnh, quá trình tách tin trong ảnh cũng được thực hiện theo các giai đoạn tương tự.

+ Đầu vào: Ảnh mang tin.
+ Đầu ra: Ảnh đã tách tin và thông điệp bí mật.

Các bước thực hiện như sau:

Bước 1: Biểu diễn ma trận điểm ảnh về dạng số thập phân với $M_c \times N_c$ phần tử. Chuyển đổi ma trận ảnh $M_c \times N_c$ phần tử về mảng 1 chiều *I* với *i* phần tử.

Bước 2: Chuyển các bit ảnh về dạng nhị phân, cứ 8 bit ảnh tách lấy *k* bit *(k* có thể là 2 hoặc 4 bit) ngoài cùng bên phải rồi ghép các kết quả này lại với nhau.

Bước 3: Kết quả thu được sử dụng hàm chuyển đổi từ chuỗi số nhị phân về chuỗi kí tự. Sau khi lặp lại quá trình trên số lần bằng số lần duyệt, thu được nội dung thông điệp.

Ví dụ dưới đây thể hiện quy trình giấu tin và tách tin bằng phương pháp giấu tin trong ảnh trên 2 LSB:

Giả sử có 4 điểm ảnh đầu tiên là: **123 197 213 255**

Chuyển các điểm ảnh về dạng nhị phân thu được kết quả tương ứng như sau:

01111011 11000101 11010101 11111111

Thông điệp bí mật *M* là chữ 'a' có mã ASCII là 97, biểu diễn dưới dạng nhị phân như sau: **01100001**

Quy trình giấu thông tin: Cứ 8 bit ảnh, lấy 6 bit đầu của điểm ảnh (từ vị trí I_0 đến I_5) ghép với 2 bit thông điệp (từ vị trí a_0 đến a_1) sẽ được:

01111001 11000110 11010100 11111101

Như vậy, ảnh sau khi giấu thông điệp M có điểm ảnh dạng nhị phân như sau:

01111001 11000110 11010100 11111101

Quy trình tách tin**:** Lấy 2 bit ngoài cùng bên phải trong mỗi điểm ảnh mới:

01111001 11000110 11010100 11111101

Ghép lại với nhau được chuỗi nhị phân thông điệp, chính là chữ "a": **0110001**

c) Nhận xét về phương pháp LSB

Dựa trên cách thức, quy trình giấu tin và tách tin sử dụng phương pháp LSB, có thể thấy phương pháp này có một số ưu điểm và nhược điểm như sau:

- *Ưu điểm:* Chất lượng hình ảnh sau giấu tin hầu như không bị ảnh hưởng. Kỹ thuật LSB đơn giản, dễ cài đặt.

- *Nhược điểm:* Tính bền vững thấp do đó thông tin mật dễ bị thay đổi do sự tác động vào hình ảnh. Bên cạnh đó, do quy trình giấu tin tương đối thô so nên thông tin mật dễ bị phát hiện bằng các phương pháp thông kê.

2.2.2. Phương pháp hoán vị giả ngẫu nhiên

Trong kỹ thuật LSB, các thông tin mật được giấu theo cách tuần tự vào các bit cố định của các khối (các điểm ảnh) liên tiếp hoặc theo trật tự nhất định. Kỹ thuật này đơn giản với người giấu tin, dễ bị tấn công vét cạn hoặc nhận dạng tự động. Để giải quyết nhược điểm này trong quá trình giấu tin thường sử dụng khóa bí mật để mã hóa thông tin cần giấu trước khi sử dụng kỹ thuật LSB hoặc áp dụng phương thức Seed (nhân). Phương thức nhân sẽ thông qua phép toán rời rạc để chọn ra các dãy điểm ảnh ngẫu nhiên thay thế việc ánh xạ tuần tự

mà LSB sử dụng. Điều này cũng giúp thông tin giấu được an toàn hơn vì để có được thông điệp, kẻ tấn công cần nắm rõ thuật toán được sử dụng trong phương thức nhân. Tiếp theo, hãy xem xét kỹ thuật giấu tin trong ảnh sử dụng phương pháp hoán vị giả ngẫu nhiên.

a) Tổng quan về phương pháp hoán vị giả ngẫu nhiên

Ý tưởng của giải pháp giấu tin trong ảnh bằng phương pháp hoán vị ngẫu nhiên chính là việc giấu thông tin vào các vị trí ngẫu nhiên, bất kỳ. Bên cạnh đó, mục đích của thuật toán cũng mong muốn tất cả các bit của ảnh chứa tin đều có thể tham gia trong quá trình giấu tin, và các bit của thông điệp cũng được phân bố ngẫu nhiên trên toàn bộ miền không gian của ảnh chứa và không tuân theo một thứ tự nào. Tuy nhiên, nếu thực hiện theo ý tưởng này thì cả người giấu tin và người tách tin đều không biết được vị trí mà các bit thông được được giấu. Chính vì vậy, phương pháp hoán vị ngẫu nhiên sẽ khó thực hiện. Để giải quyết vấn đề này, các chuyên gia đề xuất giải pháp hoán vị giả ngẫu nhiên. Theo đó, hoán vị giả ngẫu nhiên sẽ vẫn dựa trên giải pháp hoán vị ngẫu nhiên nhưng vị trí các bit được lựa chọn để giấu thông tin sẽ không phải là ngẫu nhiên nữa mà là giả ngẫu nhiên. Có nghĩa là sẽ áp dụng một kỹ thuật hoặc một thuật toán nào đó để sinh ra chuỗi ngẫu nhiên và chuỗi ngẫu nhiên này sẽ khác nhau sau mỗi lần giấu tin.

b) Giới thiệu về thuật toán hoán vị giả ngẫu nhiên

Bộ sinh số giả ngẫu nhiên (pseudorandom number generator - PRNG), còn được gọi là bộ sinh bit ngẫu nhiên tất định (DRBG) [11]. Đây là thuật toán sinh ra chuỗi các số có các thuộc tính gần như thuộc tính của chuỗi số ngẫu nhiên. Chuỗi sinh ra từ bộ sinh số giả ngẫu nhiên sẽ không thực sự là ngẫu nhiên bởi vì nó hoàn toàn được xác định từ giá trị khởi đầu, được gọi là nhân của nó. Để hiểu rõ hơn về bộ sinh số giả ngẫu nhiên, giáo trình sẽ giới thiệu một thuật toán sinh số giả ngẫu nhiên được sử dụng phổ biến – thuật toán Blum Blum Shub. Thuật toán Blum Blum Shub (B.B.S) là một thuật toán sinh số giả ngẫu nhiên được đề xuất vào năm 1986 bởi Lenore Blum, Manuel Blum và Michael Shub [12]. Thuật toán lựa chọn hai số nguyên tố lớn p và q. Hai số nguyên tố này nên thỏa mãn điều kiện sau để đảm bảo có chu kỳ dài (xem công thức 2.2):

$$\begin{cases} p \equiv q \equiv 3 \ (mod\ 4) \\ \text{gcd}\ (p, q)\ \text{là}\ nhỏ\ nhất \end{cases} \tag{2.2}$$

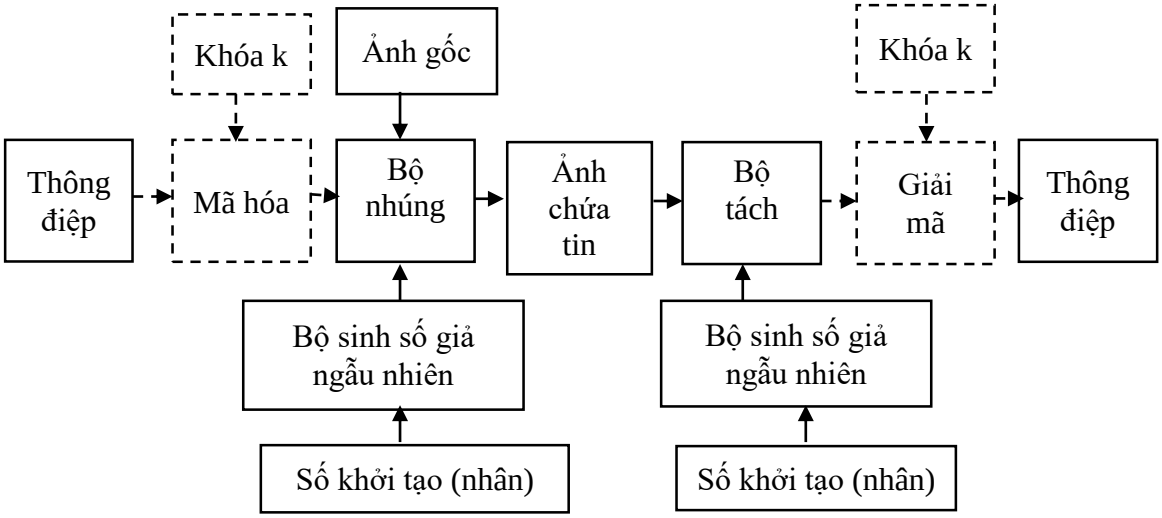
Trong đó, $p \equiv q \equiv 3 \ (mod\ 4)$ là kỹ thuật đồng dư. Để hiểu rõ hơn về nguyên tắc của kỹ thuật đồng dư người đọc có thể tìm hiểu trong tài liệu [34]. Tiếp theo, tính giá trị $M = p \times q$ và lựa chọn một nhân (số khởi tạo) x_0. Số x_0 cần đảm bảo là nguyên tố cùng nhau với số M và khác 0 hoặc 1. Khi đó các số giả ngẫu nhiên được sinh ra theo công thức 2.3:

$$x_{n+1} = x_n^2 \ mod\ M \tag{2.3}$$

Ví dụ: Lựa chọn $p = 11, q = 19\ và\ x_0 = 3$ khi đó sinh được dãy các số là $\{9, 81, 82, 36, 42, 92, \dots\}$

c) Kỹ thuật giấu tin bằng phương pháp hoán vị giả nhẫu nhiên

Hình 2.2 mô tả mô hình giấu tin và tách tin trong ảnh sử dụng phương pháp hoán vị giả ngẫu nhiên. Trong đó những nét đứt của hình và mũi tên thể hiện những quy trình này có thể sử dụng hoặc không sử dụng trong quy trình giấu tin và tách tin tùy theo người dùng lựa chọn.



Hình 2.2. Sơ đồ giấu và tách tin của phương pháp hoán vị giả ngẫu nhiên

Theo sơ đồ tổng quan về quá trình giấu và tách tin thể hiện qua hình 2.2 có thể thấy, để thực hiện giấu tin và tách tin, bên nhận và bên gửi cần thống nhất với nhau về việc sử dụng thuật toán sinh bộ số giả ngẫu nhiên và giá trị khởi tạo ban đầu hoặc gửi giá trị khởi tạo qua kênh truyền an toàn. Ngoài ra nếu thông tin được mã hóa thì hai bên cũng cần thống nhất thuật toán mã hóa, giải mã và gửi khóa qua kênh truyền an toàn.

Quy trình thực hiện giấu tin bằng phương pháp hoán vị giả ngẫu nhiên như sau:

Bước 1: Thông tin được mã hóa (nếu cần) sau đó được chuyển sang thành dãy nhị phân. Gọi l_m là độ dài của thông điệp (ở dạng nhị phân) và tương ứng m_i là bit thứ *i* của thông điệp sau khi mã hóa và chuyển về dạng nhị phân.

Bước 2: Trích xuất ma trận điểm ảnh trong ảnh, biến đổi các điểm ảnh về dạng nhị phân và chuyển ma trận thành dãy nhị phân. Gọi l_c là độ dài của ảnh sau khi chuyển về dãy nhị phân và tương ứng c_i là bit thứ *i* trong ảnh.

Bước 3: Sử dụng bộ sinh số giả ngẫu nhiên và giá trị khởi tạo chọn trước, sinh dãy số $r_1, r_2, \dots, r_{l_m}$.

Bước 4: Thay thế bit c_{r_i} của ảnh bằng bit m_i của thông tin.

Quy trình tách tin: Dựa trên 4 bước của quá trình giấu tin như trên thì quá trình tách tin cũng bao gồm các bước tiến hành và xử lý như sau:

Bước 1: Trích xuất ma trận điểm ảnh trong ảnh, biến đổi các điểm ảnh về dạng nhị phân và chuyển ma trận thành dãy nhị phân. Gọi l_c là độ dài của ảnh sau khi chuyển về dãy nhị phân và tương ứng c_i là bit thứ i trong ảnh.

Bước 2: Sử dụng bộ sinh số giả ngẫu nhiên và giá trị khởi tạo chọn trước, sinh dãy số $r_1, r_2, \dots, r_{l_m}$.

Bước 3: Lần lượt lấy ra các bit c_{r_i} của ảnh và ghép lại để được một dãy nhị phân. Đây chính là dãy nhị phân của thông điệp.

d) Nhận xét về phương pháp hoán vị giả ngẫu nhiên

Dựa trên quá trình giấu tin và tách tin được mô tả trong mục (c) ở trên có thể thấy rằng giấu tin bằng phương pháp giấu tin bằng phương pháp hoán vị giả ngẫu nhiên có độ an toàn cao. Nguyên nhân của vấn đề này là do kỹ thuật này sử dụng bộ sinh số giả ngẫu nhiên nên kẻ tấn công khó tìm được quy luật giấu tin như LSB vì các bit của thông điệp được giấu vào các bit ngẫu nhiên trong ảnh. Mặc dù vậy, phương pháp này dễ xảy ra xung đột trong quá trình nhúng khi chu kì của bộ sinh số giả ngẫu nhiên không đủ lớn (nhỏ hơn hoặc bằng l_m) sẽ dẫn đến tính trạng có nhiều hơn 1 bit được giấu vào cùng 1 vị trí. Ngoài ra, ảnh sau khi được giấu tin sẽ bị thay đổi giá trị rất nhiều do các bit thông tin được giấu vào các bit bất kì chứ không phải chỉ LSB. Điều này dẫn đến kẻ tấn công dễ dàng phát hiện ảnh đang chứa tin chỉ cần nhìn qua bằng mắt thường. Để giải quyết nhược điểm này, trong thực tế các chuyên gia thường kết hợp giữa kỹ thuật LSB với kỹ thuật hoán vị giả ngẫu nhiên. Theo đó, phương pháp hoán vị giả ngẫu nhiên sẽ sinh ra các số ngẫu nhiên và các số ngẫu nhiên này sẽ được coi là các điểm ảnh. Sau đó sẽ áp dụng kỹ thuật LSB vào để giấu thông tin và các vị trí vừa tìm được.

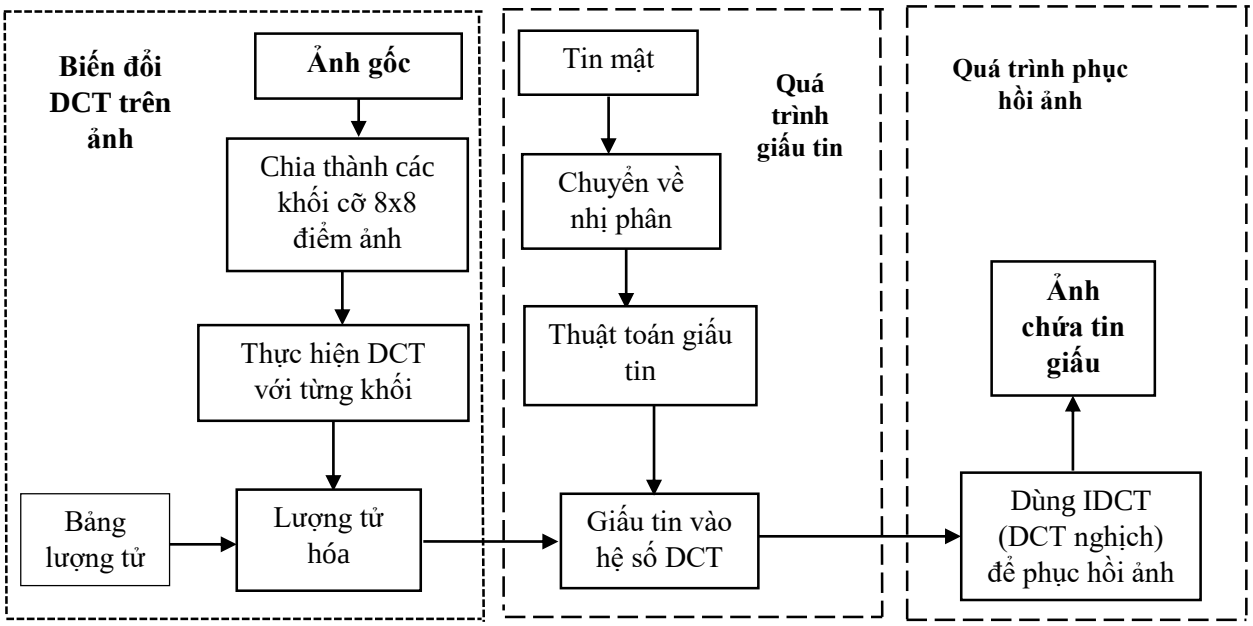
2.3. Phương pháp giấu tin trong miền tần số ảnh

2.3.1. Phương pháp giấu tin dựa trên biến đổi DCT

a) Giới thiệu phương pháp

Phương pháp giấu tin trong ảnh sử dụng kỹ thuật biến đổi miền tần số là phương pháp được ứng dụng nhiều hiện nay. Một trong những phương pháp nổi bật được sử dụng trong phương pháp biến đổi miền tần số là phương pháp biến đối cosine rời rạc (Discrete Cosine Transform- DCT). Phương pháp DCT trên ảnh là phương pháp biến đổi dữ liệu ảnh từ dạng không gian về dạng tần số [2, 5, 13, 14]. Mục đích của quá trình biến đổi là thay đổi dữ liệu biểu diễn thông tin. Theo đó, dữ liệu của ảnh con tập trung vào một phần nhỏ các hệ số hàm truyền. Hình 2.3 thể hiện các bước chính của phương pháp giấu tin trong ảnh dựa trên DCT.

Từ sơ đồ 2.3 thấy được, quá trình giấu tin trong ảnh dựa trên biến đổi DCT gồm 3 bước chính bước sau [1, 2, 5, 10, 14]: Biến đổi DCT; Giấu tin vào hệ số DCT; Phục hồi ảnh. Tiếp theo giáo trình sẽ trình bày chi tiết về các các quy trình biến đổi này



Hình 2.3. Sơ đồ tổng quan về quá trình giấu tin sử dụng DCT

b) Quy trình giấu tin

- Biến đổi DCT trên ảnh: Dựa trên mô tả trong hình 2.3 có thể thấy các khối chính trong biến đổi DCT bao gồm:

+ Khối "Chia thành các khối cỡ 8x8 điểm ảnh ": Trước tiên, vì ảnh gốc có kích thước rất lớn nên trước khi thực hiện biến đổi DCT, ảnh được phân chia thành các khối lớn riêng biệt không chồng nhau (MB- Marco Block). Mỗi MB bao gồm 4 khối các tín hiệu chói (Y) và 2; 4 hoặc 8 khối các mẫu tín hiệu màu (Cr, Cb). Tất cả các khối có cùng kích thước, mỗi khối có kích thước 8 x 8 điểm ảnh và biểu diễn các mức xám của 64 điểm ảnh [2, 5, 10, 14].

+ Khối "Thực hiện DCT với từng khối": Sau đó các giá trị trong khối ảnh phải được trừ đi cùng một giá trị để các giá trị ở trung tâm là 0. Ví dụ mỗi giá trị trong khối 8x8 có giá trị trong đoạn [0; 255] có giá trị ở chính giữa là 128. Phải lấy các giá trị trong khối trừ đi 128 để các giá trị nằm trong khoảng đoạn [-128; 127] tức là giá trị chính giữa là 0. Đây là yêu cầu của biến đổi DCT. Mỗi khối 64 điểm ảnh sau biến đổi DCT thuận sẽ nhận được 64 hệ số thực DCT. Tiếp theo các khối này sẽ được biến đổi DCT. Có 2 kỹ thuật biến đổi DCT chính bao gồm:

o *DCT một chiều:* DCT một chiều biểu diễn biên độ tín hiệu tại các thời điểm rời rạc theo thời gian hoặc không gian thành chuỗi các hệ số rời rạc, mỗi hệ số biểu diễn biên độ của một thành phần tần số nhất định có trong tín hiệu gốc. Hệ số đầu tiên biểu diễn mức DC trung bình của tín hiệu. Các hệ số thể hiện các thành phần tần số không gian cao hơn của tín hiệu và được gọi là các hệ số AC. Thông thường nhiều hệ số AC có giá trị gần hoặc bằng 0. Quá trình biến đổi DCT thuận (FDCT) được định nghĩa như công thức 2.4 sau đây:

$$X(k) = \sqrt{\frac{2}{N}} C(k) \sum_{m=0}^{N-1} x(m) \cos \frac{(2m+1)k\pi}{2N} \quad (2.4)$$

Hàm biến đổi DCT ngược (một chiều) thể hiện qua công thức 2.5:

$$x(m) = \sqrt{\frac{2}{N}} \sum_{k=0}^{N-1} X(k) C(k) \cos \frac{(2m+1)k\pi}{2N} \quad (2.5)$$

Trong đó:

$X(k)$ là chuỗi kết quả. k chỉ số của hệ số khai triển.

$x(m)$ là giá trị mẫu m. m chỉ số của mẫu.

N chỉ số mẫu có trong tín hiệu.

$$C(k) = \begin{cases} \frac{1}{\sqrt{2}} \ \text{nếu } k = 0 \\ 1 \ \text{nếu } k \neq 0 \end{cases} \quad (2.6)$$

- *DCT hai chiều:* Biến đổi DCT hai chiều (2-D) được dùng cho các khối ảnh có kích thước 8x8. Quá trình biến đổi DCT thuận được định nghĩa như sau (xem công thức 2.7) [7]:

$$F(u,v) = \frac{C(u)C(v)}{4} \sum_{j=0}^{7} \sum_{k=0}^{7} f(j,k) \cos \frac{(2j+1)u\pi}{16} \cos \frac{(2k+1)v\pi}{16} \quad (2.7)$$

Trong đó:

f(j ,k) là các mẫu của ảnh gốc trong khối 8x8 điểm ảnh.

F(u, v) là các hệ số của khối DCT 8x8

$$C(u), C(v) = \begin{cases} \frac{1}{\sqrt{2}} \ \text{nếu } u, v = 0 \\ 1 \ \text{nếu } u, v \neq 0 \end{cases} \quad (2.8)$$

Công thức 2.8 trên là kết quả của hai công thức DCT một chiều, một cho tần số ngang và một cho tần số dọc. Trong ma trận hệ số DCT hai chiều, hệ số thứ nhất *F(0,0)* bằng giá trị trung bình của các điểm ảnh trong khối 8x8 (xem công thức 2.9).

$$F(0,0) = \frac{1}{8} \sum_{j=0}^{7} \sum_{k=0}^{7} f(j,k) \quad (2.9)$$

Các hệ số nằm ở các dòng dưới thành phần một chiều đặc trưng cho các tần số cao hơn của tín hiệu theo chiều dọc. Các hệ số nằm ở các cột bên phải của thành phần một chiều đặc trưng cho các tần số cao hơn theo chiều ngang. Hệ số *F(0,7)* là thành phần có tần số cao nhất theo chiều ngang của khối ảnh 8x8 và hệ số *F(7,0)* đặc trưng cho các thành phần có tần số cao nhất theo chiều dọc. Các hệ số khác ứng với những phối hợp khác nhau của các tần số theo chiều dọc và chiều ngang. Phép biến đổi DCT hai chiều là phép biến đổi đối xứng và biến đổi nghịch cho phép tái tạo lại các giá trị mẫu *f(j, k)* trên cơ sở các hệ số *F(u,v)* theo công thức 2.10:

$$f(j,k) = \sum_{u=0}^{7}\sum_{v=0}^{7} \frac{C(u)C(v)}{4} F(u,v)\cos\frac{(2j+1)u\pi}{16}\cos\frac{(2k+1)v\pi}{16} \qquad (2.10)$$

+ Khối "Lượng tử hóa": Sau khi thực hiện biến đổi DCT, 64 hệ số sẽ được lượng tử hóa dựa trên một bảng lượng tử gồm 64 phần tử $Q(u,v)$ với $0 \le u,v \le 7$. Bảng này được định nghĩa bởi từng ứng dụng cụ thể. Các phần tử trong bảng lượng tử có giá trị từ 1 đến 255 được gọi là các bước nhảy cho các hệ số DCT. Quá trình lượng tử được coi như là việc chia các hệ số DCT cho bước nhảy lượng tử tương ứng, kết quả này sau đó sẽ được làm tròn xuống số nguyên gần nhất. Công thức dưới đây thể hiện việc lượng tử với $F(u,v)$ là các hệ số DCT, $F^Q(u,v)$ là các hệ số sau lượng tử, các hệ số này sẽ được đưa vào bộ mã hóa Huffman (xem công thức 2.11).

$$F^Q(u,v) = IntegerRound\left(\frac{F(u,v)}{Q(u,v)}\right) \qquad (2.11)$$

Mục đích của việc lượng tử hóa là giảm số lượng bit cần để lưu trữ các hệ số biến đổi bằng việc giảm độ chính xác của các hệ số này cho nên lượng tử là quá trình xử lý có mất thông tin. Một tính năng quan trọng của quá trình này là các mức độ nén và chất lượng hình ảnh khác nhau có thể đạt được qua việc lựa chọn các ma trận lượng tử cụ thể. Điều này cho phép người dùng quyết định mức chất lượng từ 1 đến 100, trong đó 1 cho chất lượng hình ảnh kém nhất và nén cao nhất, trong khi 100 cho chất lượng tốt nhất và nén thấp nhất. Kết quả là tỷ lệ chất lượng/nén có thể được điều chỉnh cho phù hợp với nhu cầu khác nhau. Các thí nghiệm chủ quan liên quan đến hệ thống thị giác con người đã dẫn đến ma trận lượng tử tiêu chuẩn. Với mức chất lượng là 50, ma trận này cho phép việc nén và giải nén đạt hiệu quả tốt nhất. Với mức lượng tử càng lớn ảnh càng được nén ít và cho hình ảnh càng rõ hơn và ngược lại. Ma trận lượng tử thu nhỏ sau đó được làm tròn và cắt bớt để có các giá trị số nguyên dương tương đương trong khoảng từ 1 đến 255. Để hiểu rõ hơn về quá trình xử lý DCT trên ảnh. Hãy xem ví dụ dưới đây:

Đầu vào: Một ma trận điểm ảnh N theo độ sáng cỡ 8x8 điểm ảnh

$$N = \begin{bmatrix} 154 & 123 & 123 & 123 & 123 & 123 & 123 & 136 \\ 192 & 180 & 136 & 154 & 154 & 154 & 136 & 110 \\ 254 & 198 & 154 & 154 & 180 & 154 & 123 & 123 \\ 239 & 180 & 136 & 180 & 180 & 166 & 123 & 123 \\ 180 & 154 & 136 & 167 & 166 & 149 & 136 & 136 \\ 128 & 136 & 123 & 136 & 154 & 180 & 198 & 154 \\ 123 & 105 & 110 & 149 & 136 & 136 & 180 & 166 \\ 110 & 136 & 123 & 123 & 123 & 136 & 154 & 136 \end{bmatrix}$$

Bước 1: Tiền xử lý ảnh. Trừ giá trị của các điểm ảnh đi 128 thu được ma trận mới M

$$M = \begin{bmatrix} 26 & -5 & -5 & -5 & -5 & -5 & -5 & 8 \\ 64 & 52 & 8 & 26 & 26 & 26 & 8 & -18 \\ 126 & 70 & 26 & 26 & 52 & 26 & -5 & -5 \\ 111 & 52 & 8 & 52 & 52 & 38 & -5 & -5 \\ 52 & 26 & 8 & 39 & 38 & 21 & 8 & 8 \\ 0 & 8 & -5 & 8 & 26 & 52 & 70 & 26 \\ -5 & -23 & -18 & 21 & 8 & 8 & 52 & 38 \\ -18 & 8 & -5 & -5 & -5 & 8 & 26 & 8 \end{bmatrix}$$

Bước 2: Biến đổi Cosin rời rạc bằng công thức 2.12 như sau:

$$D=TMT' \tag{2.12}$$

Ma trận *T* được định nghĩa theo công thức 2.13:

$$T_{i,j} = \begin{cases} \frac{1}{\sqrt{N}} & nếu\ i = 0 \\ \sqrt{\frac{2}{N}} \cos\left[\frac{(2j+1)i\pi}{16}\right] & nếu\ i > 0 \end{cases} \tag{2.13}$$

Với *i* là số hàng còn *j* là số cột

N là giá trị của số điểm ảnh tối đa. Vì đầu vào ở đây là khối 8x8 điểm ảnh nên có ma trận kết quả sau:

$$T = \begin{bmatrix} 0.3536 & 0.3536 & 0.3536 & 0.3536 & 0.3536 & 0.3536 & 0.3536 & 0.3536 \\ 0.4904 & 0.4157 & 0.2778 & 0.0975 & -0.0975 & -0.2778 & -0.4157 & -0.4904 \\ 0.4619 & 0.1913 & -0.1913 & -0.4619 & -0.4619 & -0.1913 & 0.1913 & 0.4619 \\ 0.4157 & -0.0975 & -0.4909 & -0.2778 & 0.2778 & 0.4904 & 0.0975 & -0.4157 \\ 0.3536 & -0.3536 & -0.3536 & 0.3536 & 0.3536 & -0.3536 & -0.3536 & 0.3536 \\ 0.2778 & -0.4904 & 0.0975 & 0.4157 & -0.4157 & -0.0975 & 0.4904 & -0.2778 \\ 0.1913 & -0.4619 & 0.4619 & -0.1913 & -0.1913 & 0.4619 & -0.4619 & 0.1913 \\ 0.0975 & -0.2778 & 0.4157 & -0.4904 & 0.4904 & -0.4157 & 0.2778 & -0.0975 \end{bmatrix}$$

Quá trình biến đổi DCT thu được:

$$D = \begin{bmatrix} 162.3 & 40.6 & 20.0 & 72.3 & 30.3 & 12.5 & -19.7 & -11.5 \\ 30.5 & 108.4 & 10.5 & 32.3 & 27.7 & -15.5 & 18.4 & -2.0 \\ -94.1 & -60.1 & 12.3 & -43.4 & -31.3 & 6.1 & -3.3 & 7.1 \\ -38.6 & -83.4 & -5.4 & -22.2 & -13.5 & 15.5 & -1.3 & 3.5 \\ -31.3 & 17.9 & -5.5 & -12.4 & 14.3 & -6.0 & 11.5 & -6.0 \\ -0.9 & -11.8 & 12.8 & 0.2 & 28.1 & 12.6 & 8.4 & 2.9 \\ 4.6 & -2.4 & 12.2 & 6.6 & -18.7 & -12.8 & 7.7 & 12.0 \\ -10.0 & 11.2 & 7.8 & -16.3 & 21.5 & 0.0 & 5.9 & 10.7 \end{bmatrix}$$

Nhận xét: Có thể thấy biến đổi DCT biểu diễn phổ tần số tín hiệu bằng các mẫu *f(j, k)* và bản thân phép biến đổi DCT không nén được số liệu, từ 64 mẫu nhận được 64 hệ số tương ứng. Tuy nhiên, phép biến đổi DCT thay đổi phân bố giá trị các hệ số so với phân bố các giá trị mẫu. Phép biến đổi DCT cho giá trị DC (*F*(*0, 0*)) thường lớn nhất và các hệ số trực tiếp kề nó ứng với tần số thấp có giá trị nhỏ hơn, các hệ số còn lại ứng với tần số cao có giá trị rất nhỏ. Khối hệ số DCT có thể chia làm 3 miền tần số thấp, miền tần số cao và miền tần số

giữa. Miền tần số thấp chứa các thông tin quan trọng ảnh hưởng đến tri giác. Miền tần số cao thường không mang tính tri giác cao. Tiếp theo các kết quả này kết hợp với bảng lượng tử hóa Q cho trước. Giáo trình sẽ sử dụng chọn ma trận lượng tử hóa là Q_{50} như sau:

$$Q_{50} = \begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix}$$

Lượng tử hóa đạt được bởi việc chia mỗi phần tử trong ma trận D cho ma trận Q, sau đó lấy giá trị gần nhất (Ví dụ: 1,2 thành 1 và 1,8 thành 2). Dùng công thức Huffman ở trên với đầu vào là 2 ma trận D và Q (xem hình 2.4).

$$\mathrm{C_{i,j}} = \mathrm{round}\left(\frac{\mathrm{D_{i,j}}}{\mathrm{Q_{i,j}}}\right) \tag{2.14}$$

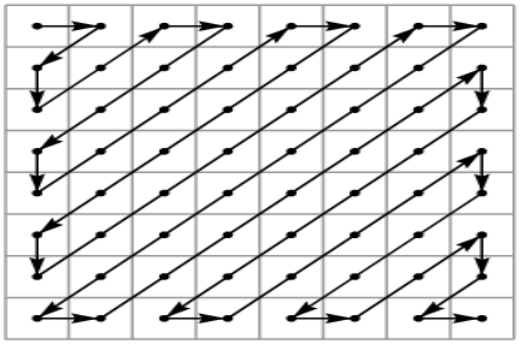
Kết quả thu được sau bước lượng tử như sau:

$$C_{50} = \begin{bmatrix} 10 & 4 & 2 & 5 & 1 & 0 & 0 & 0 \\ 3 & 9 & 1 & 2 & 1 & 0 & 0 & 0 \\ -7 & -5 & 1 & -2 & -1 & 0 & 0 & 0 \\ -3 & -5 & 0 & -1 & 0 & 0 & 0 & 0 \\ -2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Quá trình giải lượng tử ở phía bộ giải mã được thực hiện ngược lại. Các hệ số sau bộ giải mã Huffman sẽ nhân với các bước nhảy trong bảng lượng tử. Kết quả này sau đó sẽ được đưa vào biến đổi DCT ngược.

- Phương pháp giấu tin: Đối với ảnh JPEG, dữ liệu gốc là các bảng DCT sau khi được lượng tử hóa. Mỗi bảng DCT chứa 64 hệ số, mỗi hệ số là số nguyên có giá trị nằm trong đoạn [-2048; 2047]. Miền tần số cao thường có nhiều giá trị 0 liên tiếp nhau, nếu giấu tin vào đây thì có thể làm tăng kích thước của ảnh do chuỗi dài số 0 bị ngắt làm giảm khả năng nén ảnh. Đặc điểm của bảng DCT là càng về cuối của bảng thì giá trị có xu hướng nhỏ dần. Có nhiều thuật toán khác nhau có thể áp dụng để giấu tin vào hệ số DCT như: LSB, Jsteg, F3, F4, Pixel Swap Embedding… Để lựa chọn thuật toán giấu tin làm ví dụ minh họa, tác giả lựa chọn thuật toán LSB. Dựa trên quá trình tính toán và xử lý tại bước biến đổi DCT, giáo trình trình bày ví dụ về quá trình giấu tin sử dụng phương pháp LSB như sau: Đầu vào: Các hệ số DCT đã được lượng tử hóa. Trong ví dụ này lựa chọn: C_{50} đã thu được ở bước trên. Thông điệp giấu: 010. Đầu ra: Ảnh có chứa thông điệp. Quá trình xử lý: Do ảnh dùng để giấu tin sẽ có kích thước lớn và bao gồm nhiều khối 8x8 điểm ảnh từ đó được nhiều ma

trận sau lượng tử *C* khác nhau và nội dung tin giấu sẽ dài và nhiều kí tự. Thông thường người giấu tin sẽ tách chuỗi tin cần giấu ra các kí tự và giấu một kí tự vào mỗi ma trận C_i . Tuy nhiên, vì không chắc chắn được tọa độ DC trong mỗi ma trận C_i là như nhau nên cần tìm ra các LSB của bit đó, để tìm được thì ma trận C_i sẽ áp dụng thuật toán *zigzac* bản chất là một thuật toán trải thẳng (biến ma trận 2 chiều thành 1 chiều) ma trận C_i theo thứ tự sau:



Hình 2.4. Thuật toán zigzac

Áp dụng thuật toán này cho ma trận C_{50} trải thẳng xong thì 3 điểm ảnh cuối cùng của dãy sẽ ứng với số 0 trong ma trận C_{50} thuộc phần DC là phần có thể giấu tin vì thế người giấu tin sẽ đổi giá trị 3 điểm ảnh này bằng 3 bit của bản rõ ban đầu (010). Kết quả giấu tin bằng thuật toán LSB như sau:

$$C_{50LSB} = \begin{bmatrix} 10 & 4 & 2 & 5 & 1 & 0 & 0 & 0 \\ 3 & 9 & 1 & 2 & 1 & 0 & 0 & 0 \\ -7 & -5 & 1 & -2 & -1 & 0 & 0 & 0 \\ -3 & -5 & 0 & -1 & 0 & 0 & 0 & 0 \\ -2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{0} \\ 0 & 0 & 0 & 0 & 0 & 0 & \mathbf{1} & \mathbf{0} \end{bmatrix}$$

- Phục hồi ảnh: Sau khi đã giấu thông tin và các hệ số của bảng lượng tử hóa. Người giấu tin sẽ tiến hành phục hồi lại ảnh sử dụng công thức tổng quát như sau (xem công thức 2.15):

$$R_{i,j} = Q_{i,j} \text{ x } C_{i,j} \qquad (2.15)$$

Trong đó $Q_{i,j}$ là ma trận lượng tử.

$C_{i,j}$ là kết quả của ma trận lượng tử đã được giấu tin

Cuối cùng thực hiện IDCT ma trận $R_{i,j}$ sẽ thu được ảnh mới theo công thức 2.16:

$$N_{i,j} = round(T'R\ T) + 128 \qquad (2.16)$$

Tiếp tục ví dụ ở trên, sau khi giấu tin xong thu được ma trận điểm ảnh R như sau:

$$R = \begin{bmatrix} 160 & 44 & 20 & 80 & 24 & 0 & 0 & 0 \\ 36 & 108 & 14 & 38 & 26 & 0 & 0 & 0 \\ -98 & -65 & 16 & -48 & -40 & 0 & 0 & 0 \\ -42 & -85 & 0 & -29 & 0 & 0 & 0 & 0 \\ -36 & 22 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 103 & 0 \end{bmatrix}$$

Thực hiện thực hiện IDCT ma trận R sẽ thu được ảnh mới là:

$$Nnew = \begin{bmatrix} 151 & 129 & 124 & 114 & 119 & 130 & 123 & 130 \\ 198 & 181 & 127 & 149 & 161 & 137 & 148 & 119 \\ 261 & 176 & 175 & 158 & 175 & 185 & 111 & 119 \\ 235 & 208 & 125 & 176 & 193 & 137 & 148 & 97 \\ 197 & 126 & 156 & 145 & 163 & 183 & 118 & 146 \\ 123 & 142 & 105 & 151 & 168 & 146 & 188 & 163 \\ 115 & 106 & 139 & 122 & 134 & 171 & 154 & 171 \\ 109 & 131 & 123 & 116 & 120 & 136 & 152 & 133 \end{bmatrix}$$

Nếu so sánh 2 ma trận điểm ảnh *N* và *Nnew* thì sẽ thấy có rất ít thông tin bị thay đổi giữa *N* và *Nnew*.

c) Quy trình tách tin

Quá trình tách tin được thực hiện tương tự như quá trình giấu tin. Theo đó, các bước tiến hành để tách tin trong ảnh sử dụng kỹ thuật DCT như sau:

- Bước 1: Đọc và thực hiện biến đổi DCT: Đọc ảnh chứa dữ liệu giấu tin, sau đó thực hiện biến đổi DCT lên ảnh này để chuyển đổi sang miền hệ số DCT. Biến đổi DCT sẽ tạo ra các hệ số DCT tương ứng với các tần số khác nhau trong ảnh.

- Bước 2: Xác định vị trí chứa dữ liệu giấu tin: tại bước này, người tách tin sẽ lựa chọn một số hệ số DCT để xác định vị trí chứa dữ liệu giấu tin, thường là các hệ số DCT có tần số thấp (gần với gốc tọa độ (0,0)). Sau đó, đối với mỗi hệ số DCT được chọn, trích xuất bit LSB (Least Significant Bit) của giá trị hệ số DCT này.

- Bước 3: Tái tạo dữ liệu giấu tin. Ghép các bit LSB trích xuất từ các hệ số DCT lại với nhau để tái tạo dữ liệu giấu tin. Có thể sử dụng các kỹ thuật như đọc từng bit trong một dãy bit và ghép lại để tái tạo dữ liệu giấu tin ban đầu.

d) Nhận xét về phương pháp

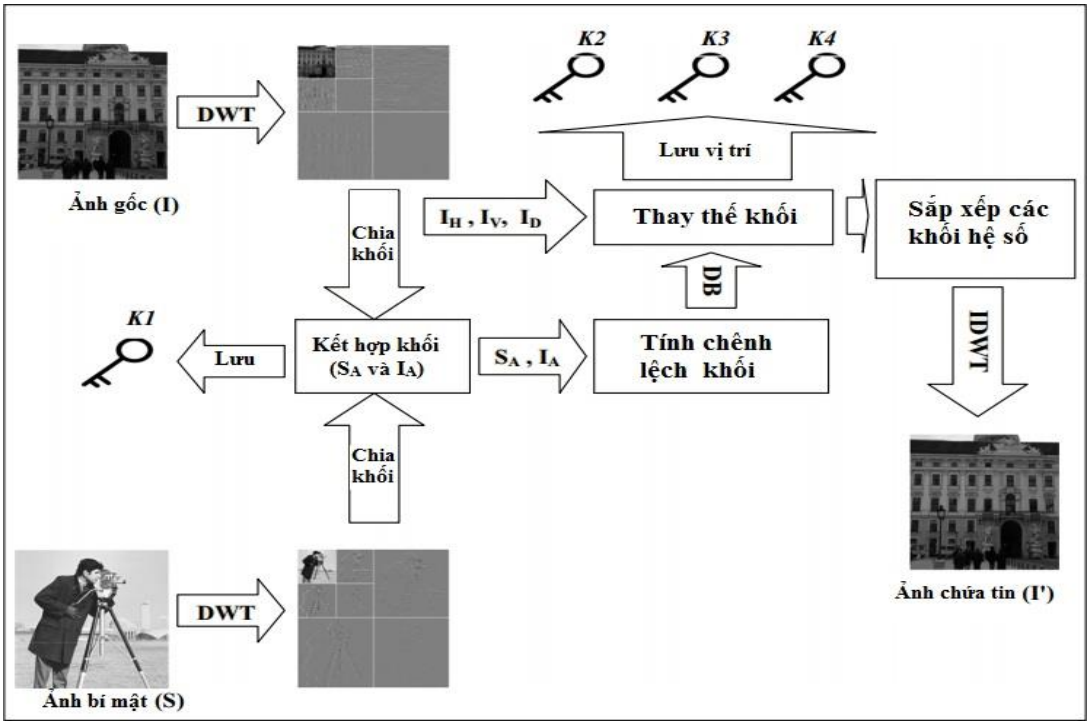
Phương pháp giấu tin trong ảnh dựa trên biến đổi miền tần số DCT là một trong những phương pháp phổ biến nhất hiện nay. Phương pháp này có ưu điểm là giấu được nhiều thông tin mà vẫn đảm bảo được chất lượng hình ảnh tốt. Trong nghiên cứu [2] đã chỉ ra rằng, phương pháp này có khả năng giảm kích thước tệp ảnh đến 90% mà vẫn giữ được chất lượng hình ảnh tương đối tốt. Ngoài ra, về mặt lý thuyết phương pháp này có quá trình tính toán đơn giản, nhanh chóng do đó rất dễ dàng thực hiện giấu tin và tách tin. Tuy nhiên, phương pháp biến đổi miền tần số DCT cũng có một số hạn chế nhất định. Cụ thể phương pháp này

không mang lại hiệu quả tốt khi áp dụng cho các tình huống khi kích thước ảnh thay đổi liên tục. Bên cạnh đó, việc sử dụng ma trận lượng tử hóa để giảm kích thước ảnh dẫn đến một số ảnh hưởng đến chất lượng nén.

2.3.2. Phương pháp giấu tin dựa trên biến đổi DWT

a) Tổng quan chung

Kỹ thuật biến đổi Wavelet rời rạc (Discrete Wavelet Transformation - DWT) là ứng dụng mới trong các ứng dụng của wavelet. DWT cung cấp cả thông tin về thời gian cũng như không gian của vật chứa. Chính điều này đã giải quyết được một số nhược điểm gặp phải của kỹ thuật DFT hoặc vấn đề giả tạo (artifact problems) của DCT. Đối với lĩnh vực giấu tin trong ảnh, DWT thực hiện trên miền tần số, mục đích của phép biến đổi nhằm thực hiện thay đổi hệ số chuyển đổi của ảnh chứa, sau đó thực hiện chuyển đổi ngược lại để thu được ảnh đã được giấu tin. Hình 2.5 mô tả quy trình giấu tin trong ảnh sử dụng kỹ thuật DWT.



Hình 2.5. Quy trình giấu tin trong ảnh sử dụng kỹ thuật biến đổi DWT

Từ hình 2.5 có thể thấy quy trình giấu tin trong ảnh dựa trên kỹ thuật DWT sẽ bao gồm hai giai đoạn chính bao gồm [1, 5, 10, 14, 15]: giấu tin vào ảnh; phục hồi ảnh. Tiếp theo, giáo trình sẽ trình bày chi tiết về hai quá trình xử lý này.

b) Quy trình giấu tin

- Phương pháp giấu tin: Mục đích của quá trình này nhằm giấu tin vào trong các hệ số tương ứng các ảnh phụ của ảnh gốc bằng cách thay thế các khối điểm ảnh trong ảnh phụ lưu hệ số bằng các khối lưu sự chênh lệch khối giữa ảnh gốc và ảnh bí mật. Dựa trên hình

2.5 có thể thấy rằng sẽ có 3 khối xử lý chính giai đoạn này bao gồm: Biến đổi DWT; Chia khối (Blocking); Kết hợp khối (Matching). Chi tiết quá trình xử lý trong từng khối như sau:

+ Biến đổi DWT: Biến đổi DWT là quá trình xử lý cả vật chứa và tin giấu. Quá trình xử lý này được thực hiện trên cả không gian và thời gian. Quy trình biến đổi DWT được thực hiện theo hai bước như sau:

- Bước 1: Thực hiện quét các điểm ảnh từ trái sang phải theo chiều ngang. Sau đó thực hiện phép cộng và phép trừ trên các điểm ảnh lân cận. Lưu trữ tổng ở bên trái và hiệu ở bên phải. Sau đó lặp lại quá trình tới khi tất cả các dòng được xử lý. Điểm ảnh tổng đại diện cho phần tần số thấp (*L*) và điểm ảnh hiệu đại diện cho phần tần số cao (*H*).
- Bước 2: Quét các điểm ảnh từ trên xuống dưới theo chiều dọc. Thực hiện phép cộng và phép trừ trên các điểm ảnh lân cận và lưu trữ tổng phía trên, hiệu ở phía dưới. Sau đó lặp lại quá trình tới khi tất cả các cột được xử lý. Cuối cùng thu được 4 dải tần phụ được biểu hiện là *LL, LH, HL, HH* tương ứng. Dải *LL* là phần tần số thấp và do đó trông rất giống với hình ảnh ban đầu.

Sau khi thực hiện biến đổi DWT, từ ảnh gốc *I* thu được 4 ảnh phụ (I_A, I_H, I_v, I_D) tương ứng. Trong đó: I_A - hệ số xấp xỉ; I_H - hệ số chi tiết chiều ngang; I_V - hệ số chi tiết chiều dọc; I_D - hệ số chi tiết đường chéo. Tương tự, sau khi biến đổi DWT, từ ảnh bí mật *S* thu được 4 ảnh phụ (S_A, S_H, S_v, S_D) tương ứng. Trong đó: S_A - hệ số xấp xỉ; S_H - hệ số chi tiết chiều ngang; S_V - hệ số chi tiết chiều dọc; S_D - hệ số chi tiết đường chéo. Một điểm cần lưu ý trong quá trình này là các ảnh phụ S_A, S_H, S_v, S_D được phân chia thành các khối không chồng nhau. Hình 2.6 thể hiện một ví dụ về sự khác biệt giữa ảnh gốc và ảnh đã được xử lý bằng DWT.

Hình 2.6. Hình ảnh gốc so với ảnh đã biến đổi DWT

Ví dụ dưới đây sẽ mô tả chi tiết một quá trình tính toán và xử lý của DWT ở trên. Theo đó, như trên hình 2.5 sẽ có hai đầu vào cần xử lý là vật chứa I dưới dạng ma trận điểm ảnh 8x8 là:

$$I = \begin{bmatrix} 154 & 123 & 123 & 123 & 123 & 123 & 123 & 136 \\ 192 & 180 & 136 & 154 & 154 & 154 & 136 & 110 \\ 254 & 198 & 154 & 154 & 180 & 154 & 123 & 123 \\ 239 & 180 & 136 & 180 & 180 & 166 & 123 & 123 \\ 180 & 154 & 136 & 167 & 166 & 149 & 136 & 136 \\ 128 & 136 & 123 & 136 & 154 & 180 & 198 & 154 \\ 123 & 105 & 110 & 149 & 136 & 136 & 180 & 166 \\ 110 & 136 & 123 & 123 & 123 & 136 & 154 & 136 \end{bmatrix}$$

Và ảnh bí mật *S* dưới dạng ma trận 4x4 như sau:

$$S = \begin{bmatrix} 224 & 154 & 125 & 238 \\ 042 & 025 & 057 & 128 \\ 163 & 123 & 242 & 234 \\ 224 & 126 & 032 & 135 \end{bmatrix}$$

Dựa trên lý thuyết ở trên, cần phải tính toán và đưa ra kết của các ảnh phụ I_A, I_H, I_V, I_D, S_A.

+ Biến đổi ảnh chứa *I*:

- Biến đổi chiều ngang

$$I_n = \begin{bmatrix} 277 & 246 & 246 & 259 & 031 & 000 & 000 & -13 \\ 372 & 290 & 308 & 246 & 012 & -18 & 000 & 026 \\ 452 & 308 & 334 & 246 & 056 & 000 & 026 & 000 \\ 419 & 316 & 346 & 246 & 059 & -44 & 014 & 000 \\ 334 & 303 & 315 & 272 & 026 & -31 & 017 & 000 \\ 264 & 259 & 334 & 352 & -08 & -13 & -26 & 044 \\ 228 & 259 & 272 & 346 & 018 & -39 & 000 & 014 \\ 246 & 246 & 259 & 290 & -26 & 000 & -13 & 018 \end{bmatrix}$$

- Biến đổi chiều dọc

$$I_D = \begin{bmatrix} 649 & 536 & 554 & 505 & 043 & -18 & 000 & 013 \\ 871 & 624 & 680 & 492 & 115 & -44 & 040 & 000 \\ 598 & 562 & 649 & 624 & 018 & -44 & -09 & 044 \\ 474 & 505 & 531 & 636 & -08 & -39 & -13 & 032 \\ -95 & -44 & -62 & 013 & 019 & 018 & 000 & -39 \\ 033 & -08 & -12 & 000 & -03 & 044 & 012 & 000 \\ 070 & 044 & -19 & -80 & 034 & -18 & 043 & -44 \\ -18 & 013 & 013 & 056 & 044 & -39 & 013 & -04 \end{bmatrix}$$

Thu được ảnh phụ I_A

$$I_A = \begin{bmatrix} 649 & 536 & 554 & 505 \\ 871 & 624 & 680 & 492 \\ 598 & 562 & 649 & 624 \\ 474 & 505 & 531 & 636 \end{bmatrix}$$

Ảnh phụ I_H

$$I_H = \begin{bmatrix} -95 & -44 & -62 & 013 \\ 033 & -08 & -12 & 000 \\ 070 & 044 & -19 & -80 \\ -18 & 013 & 013 & 056 \end{bmatrix}$$

Ảnh phụ I_V

$$I_V = \begin{bmatrix} 043 & -18 & 000 & 013 \\ 115 & -44 & 040 & 000 \\ 018 & -44 & -09 & 044 \\ -08 & -39 & -13 & 032 \end{bmatrix}$$

Ảnh phụ I_D

$$I_D = \begin{bmatrix} 019 & 018 & 000 & -39 \\ -03 & 044 & 012 & 000 \\ 034 & -18 & 043 & -44 \\ 044 & -39 & 013 & -04 \end{bmatrix}$$

+ Biến đổi ảnh bí mật S

- Biến đổi chiều ngang

$$S_H = \begin{bmatrix} 378 & 363 & 070 & -113 \\ 067 & 185 & 017 & -71 \\ 286 & 476 & 040 & 008 \\ 350 & 167 & 098 & -103 \end{bmatrix}$$

- Biến đổi chiều dọc

$$S_D = \begin{bmatrix} 445 & 548 & 087 & -184 \\ 636 & 643 & 138 & -95 \\ 311 & 178 & 053 & -42 \\ -64 & 309 & -58 & 111 \end{bmatrix}$$

Thu được ảnh phụ S_A

$$S_A = \begin{bmatrix} 445 & 548 \\ 636 & 643 \end{bmatrix}$$

+ Chia khối: Tại bước này, các ảnh phụ cần được xử lý theo khối nhằm thực hiện cho việc thay thế khối ở bước sau. Các ảnh phụ S_A, I_A, I_H, I_v, I_D, thành các khối 4x4 điểm ảnh như sau:

$$S_A = \{B_{SAi},\ 1 \le i \le S_{An}\}$$
$$I_A = \{B_{IAj},\ 1 \le j \le I_{An}\}$$
$$I_H = \{B_{IHk},\ 1 \le k \le I_{Hn}\}$$
$$I_V = \{B_{IVl},\ 1 \le l \le I_{Vn}\}$$
$$I_D = \{B_{IDp},\ 1 \le p \le I_{Dn}\}$$

Với S_{An}, I_{An}, I_{Hn}, I_{vn}, I_{Dn} lần lượt là tổng số khối mà các ảnh S_A, I_A, I_H, I_v, I_D được chia tương ứng. B_{SAi}, B_{IAj}, B_{Ihk}, B_{IVl}, B_{Idp} lần lượt là các khối thứ i, j, k, l, p tương ứng của các ảnh phụ S_A, I_A, I_H, I_v, I_D.

Tiếp tục ví dụ về quá trình tính toán ở trên, với đầu vào là các ảnh phụ S_A, I_A, I_H, I_V, I_D thu được ở bước biến đổi DWT. Cần phải tính toán các khối ảnh của từng ảnh phụ. Quá trình biến đổi như sau:

+ Ảnh phụ I_A được chia thành các khối B_{IA1}, B_{IA2}, B_{IA3}, B_{IA4}:

B_{IA1}	B_{IA2}	B_{IA3}	B_{IA4}
649 536 871 624	598 562 474 505	649 624 531 636	554 505 680 492

+ Ảnh phụ I_H được chia thành các khối B_{IH1}, B_{IH2}, B_{IH3}, B_{IH4}

B_{IH1}	B_{IH2}	B_{IH3}	B_{IH4}
−95 −44 033 −08	−62 013 −12 000	070 044 −18 013	−19 −80 013 056

+ Ảnh phụ I_V được chia thành các khối B_{IV1}, B_{IV2}, B_{IV3}, B_{IV4}

B_{IV1}	B_{IV2}	B_{IV3}	B_{IV4}
043 −18 115 −44	000 013 040 000	018 −44 −08 −39	−09 044 −13 032

+ Ảnh phụ I_D được chia thành các khối B_{ID1}, B_{ID2}, B_{ID3}, B_{ID4}

B_{ID1}	B_{ID2}	B_{ID3}	B_{ID4}
019 018 −03 044	000 −39 012 000	034 −18 044 −39	043 −44 013 −04

+ Ảnh phụ S_A gồm 4x4 điểm ảnh nên không cần thực hiện chia, khối ảnh B_{SA} là S_A

$$B_{SA} = \begin{bmatrix} 445 & 548 \\ 636 & 643 \end{bmatrix}$$

+ Kết hợp khối: Đây là quá trình giấu tin vào trong ảnh. Quá trình giấu tin được thực hiện bằng cách thay thế các khối ảnh. Theo đó, các khối ảnh gốc sẽ được thay thế bằng các khối ảnh cần giấu. Để thực hiện được mục tiêu đề ra cần tìm các khối ảnh có sai khác nhỏ nhất nhằm đảm bảo việc giấu tin không gây thay đổi quá lớn tới ảnh. Với mỗi khối B_{SAi} trong S_A, khối B_{IAj} có lỗi nhỏ nhất trong I_A được tìm sử dụng bằng phương pháp căn bậc hai của mức trung bình của các sai số bình phương (Root Mean Square Error (RMSE) được gọi là khối phù hợp nhất (best match)). Khóa bí mật K_1 chứa các địa chỉ j của các khối B_{IAi} có lỗi nhỏ nhất được lưu lại. Ví dụ: Khối B_{SA5} có khối phù hợp nhất là khối B_{IA6}, khối B_{SA6} có khối phù hợp nhất là khối B_{IA12}, vậy khóa K_1 sẽ là (6,12). Khối có lỗi nhỏ nhất là khối có điểm khác biệt ít nhất so với các khối còn lại trong ảnh, đối với khối được dùng để so sánh.

Để hiểu rõ hơn về quá trình thay thế này, hãy tiếp tục với kết quả của các quá trình tính toán khối ở trên. Theo đó, với đầu vào là các khối B_{IA} của I_A và các khối B_{SA} của $S_{A.}$ cần tính toán để có được khóa K_1 lưu các vị trí của các khối thích hợp nhất trong các khối B_{IA} với các khối B_{SA} tương ứng. Để tìm khối phù hợp nhất với B_{SA} sử dụng phương pháp RMSE [15]. Các giá trị RMSE của từng cặp tính được như sau;

RMSE (B_{SA}, B_{IA1}) = 156.002

RMSE (B_{SA}, B_{IA2}) = 131.237

RMSE (B_{SA}, B_{IA3}) = 120.898

RMSE (B_{SA}, B_{IA4}) = 98.065

Từ các kết quả trên có thể thấy RMSE (B_{SA}, B_{IA2}) có giá trị thấp nhất, vậy nên khối B_{IA4} là khối phù hợp nhất với B_{SA}. Lúc này khóa K_1 lưu giá trị 4 - vị trí khối B_{IA4}

- Phục hồi ảnh: Quá trình phục hồi ảnh chứa tin giấu sẽ bao gồm bốn khối chính là: Tính chênh lệch khối (Difference Blocks Computation); Thay thế khối (Block Replacement); Sắp xếp các khối hệ số (Rearrangment of Coefficients Blocks). Biến đổi DWT ngược. Trong đó:

+ Tính chênh lệch khối: thực hiện tính toán được khối chênh lệch DB_i để sử dụng thay thế vào vị trí các khối phù hợp nhất nằm trong các ảnh phụ I_V, I_H, I_D. Quá trình tính giá trị chênh lệch khối DB_i giữa khối B_{SAi} và khối phù hợp nhất B_{IAj} theo công thức sau (xem công thức 2.17):

$$DB_i = B_{SAi} - (\min_{1 \le j \le IAn} B_{IAj}) \quad (2.17)$$

Ví dụ với đầu vào là các khối B_{SAi} và các khối B_{IAj} phù hợp nhất tương ứng thu được tại bước kết hợp khối ở trên thì đầu ra cần tính độ chênh lệch khối DB_i tương ứng các cặp B_{SAi} B_{IAj} này. Do B_{SA} thu được ở trên chỉ có duy nhất một khối nên chỉ cần thực hiện tính toán cho một khối đó:

$$DB = B_{SA} - B_{IA4} = \begin{bmatrix} 445 & 548 \\ 636 & 643 \end{bmatrix} - \begin{bmatrix} 554 & 505 \\ 680 & 492 \end{bmatrix} = \begin{bmatrix} -109 & 043 \\ -44 & 151 \end{bmatrix}$$

+ Thay thế khối: nguyên tắc giấu tin ảnh thông qua thay thế các khối chênh lệch với các khối được lựa chọn nhằm đảm bảo thay đổi sau khi giấu tin là thấp nhất. Với mỗi khối chênh lệch DB_i, thực hiện tìm khối phù hợp nhất B_{IHk} trong I_H bằng thuật toán RMSE. Tương tự thực hiện tìm khối phù hợp nhất B_{IVl} trong I_H, tìm khối phù hợp nhất B_{IDp} bằng thuật toán RMSE. Quá trình thực hiện được mô tả qua công thức 2.18, 2.19, 2.20:

$$B_{tCH} = \min_{1 \le k \le IHn} (\text{RMSE } (DB_i, B_{IHk})) \quad (2.18)$$

$$B_{tCV} = \min_{1 \le l \le IVn} (\text{RMSE } (DB_i, B_{IVl})) \quad (2.19)$$

$$B_{tCD} = \min_{1 \le p \le IDn} (\text{RMSE } (DB_i, B_{IDp})) \quad (2.20)$$

Thay thế DB_i vào khối thích hợp nhất trong các khối B_{tCH}, B_{tCV}, B_{tCD}. Các khóa K_2, K_3, K_4 chứa các địa chỉ k, l, p tương ứng với các khối B_{tCH}, B_{tCV}, B_{tCD}

$$DB_i \leftarrow \min \{ B_{tCH}, B_{tCV}, B_{tCD} \}$$

Để hiểu rõ hơn về các phép tính toán và biến đổi trong bước thay thế khối. Hãy xem xét ví dụ dưới đây. Với đầu vào là các khối chênh lệch DB_i, các khối của ảnh phụ I_H, I_V, I_D thu được ở trên. Cần tìm các khóa K_2, K_3, K_4 lưu vị trí các khối phù hợp nhất với DB_i tương ứng trong các khối B_{IHk}, B_{IVl}, B_{IDp} của ảnh phụ I_H, I_V, I_D. Trước tiên, cần tính toán RMSE để tìm khối phù hợp nhất với khối DB trong các khối B_{IH}. Theo lý thuyết ở trên sẽ thu được các kết quả RMSE như sau:

RMSE (DB, B_{IH1}) = 98.710

RMSE (DB, B_{IH2}) = 82.058

RMSE (DB, B_{IH3}) = 113.756

RMSE (DB, B_{IH4}) = 94.211

Vậy khối B_{IH2} phù hợp với DB nhất trong các khối của I_H.

Tiếp tục thực hiện tính khối phù hợp nhất với khối DB trong các khối B_{IV}

RMSE (DB, B_{IV1}) = 150.109

RMSE (DB, B_{IV2}) = 103.245

RMSE (DB, B_{IV3}) = 123.586

RMSE (DB, B_{IV4}) = 79.251

Vậy khối B_{IV4} phù hợp với DB nhất trong các khối của I_V

Tương tự như vậy, thực hiện tính khối phù hợp nhất với khối DB trong các khối B_{ID}

RMSE (DB, B_{ID1}) = 86.803

RMSE (DB, B_{ID2}) = 105.525

RMSE (DB, B_{ID3}) = 130.398

RMSE (DB, B_{ID4}) =120.361

Vậy: Khối B_{ID1} phù hợp với DB nhất trong các khối của I_D

Tiếp theo, cần tìm khối phù hợp nhất với khối DB trong 3 khối B_{IH2}, B_{IV4}, B_{ID1} vừa tìm được. Từ các kết quả trên thấy rằng: Khối B_{IV4} phù hợp nhất với RMSE (DB, B_{IV4}) = 79.251 vì kết quả thấp nhất. Kết luận: khóa K_3 lưu cặp giá trị (1, 4) tương ứng i=1 và k=4. Cuối cùng, thực hiện thay thế DB vào vị trí B_{IV4}, B_{IV4} thu được $\begin{bmatrix} -109 & 043 \\ -44 & 151 \end{bmatrix}$

+ Sắp xếp các khối hệ số: Sau khi thực hiện thay thế các khối, tại khối này cần sắp xếp lại các khối theo đúng thứ tự. Theo ví dụ ở trên, với đầu vào là các khối hệ số B_{IHk}, B_{IVl}, B_{IDp} của ảnh phụ I_H, I_V, I_D sau khi giấu khối chênh lệch bằng cách thay thế. Khối này sẽ phải sắp xếp các ảnh phụ được theo đúng vị trí thứ tự các khối. Vì chỉ thực hiện giấu DB vào một khối là B_{IV4} nên khối này chỉ cần phần sắp xếp cho ảnh I_V tương ứng:

Các khối của ảnh phụ I_V sau khi giấu:

$\begin{matrix}043 & -18\\ 115 & -44\end{matrix}$	$\begin{matrix}000 & 013\\ 040 & 000\end{matrix}$	$\begin{matrix}018 & -44\\ -08 & -39\end{matrix}$	$\begin{matrix}-109 & 043\\ -44 & 151\end{matrix}$
B_{IV1}	B_{IV2}	B_{IV3}	B_{IV4}

Ảnh phụ I_V sau khi đưa về đúng vị trí:

$$\begin{bmatrix}043 & -18 & 000 & 013\\ 115 & -44 & 040 & 000\\ 018 & -44 & -109 & 043\\ -08 & -39 & -44 & 151\end{bmatrix}$$

+ Thực hiện DWT ngược: Mục đích của quá trình DWT ngược là đưa ảnh từ các ảnh phụ trở về ảnh toàn vẹn chứa tin đã giấu. Cách thức thực hiện DWT có trình tự ngược với DWT (thực hiện theo chiều dọc trước, chiều ngang sau) và triển khai bằng cách tìm giá trị 2 số khi biết tổng và hiệu. Ví dụ dưới đây mô tả quy trình biến đổi DWT ngược:

Đầu vào: Các ảnh phụ I_A, I_H, I_V, I_D đã được giấu tin. Đầu ra: Ảnh I' đã chứa tin giấu. Vì chỉ có ảnh phụ I_H thay đổi sau quá trình giấu nên các ảnh I_A, I_V, I_D giữ nguyên, còn ảnh I_H thay đổi với ma trận điểm ảnh được trình bày ở bước trước.

- Ảnh I_A

$$\begin{bmatrix}599 & 536 & 554 & 505\\ 871 & 624 & 680 & 492\\ 598 & 562 & 649 & 624\\ 474 & 505 & 531 & 636\end{bmatrix}$$

- Ảnh I_H

$$\begin{bmatrix}-95 & -44 & -62 & 013\\ 033 & -08 & -12 & 000\\ 070 & 044 & -19 & -80\\ -18 & 013 & 013 & 056\end{bmatrix}$$

- Ảnh I_V

$$\begin{bmatrix}043 & -18 & 000 & 013\\ 115 & -44 & 040 & 000\\ 018 & -44 & -109 & 043\\ -08 & -39 & -44 & 151\end{bmatrix}$$

- Ảnh I_D

$$\begin{bmatrix}019 & 018 & 000 & -39\\ -03 & 044 & 012 & 000\\ 008 & -44 & -09 & -44\\ 044 & -39 & 013 & -04\end{bmatrix}$$

- Sắp xếp các ảnh theo đúng vị trí thu được ma trận điểm ảnh:

$$\begin{bmatrix} 649 & 536 & 554 & 505 & 043 & -18 & 000 & 013 \\ 871 & 624 & 680 & 492 & 115 & -44 & 040 & 000 \\ 598 & 562 & 649 & 624 & 018 & -44 & -109 & 043 \\ 474 & 505 & 531 & 636 & -08 & -39 & -44 & 151 \\ -95 & -44 & -62 & 013 & 019 & 018 & 000 & -39 \\ 033 & -08 & -12 & 000 & -03 & 044 & 012 & 000 \\ 070 & 044 & -19 & -80 & 034 & -18 & 043 & -44 \\ -18 & 013 & 013 & 056 & 044 & -39 & 013 & -04 \end{bmatrix}$$

- Thực hiện DWT đảo theo chiều dọc

$$\begin{bmatrix} 277 & 246 & 246 & 259 & 031 & 000 & 000 & -13 \\ 372 & 290 & 308 & 246 & 012 & -18 & 000 & 026 \\ 452 & 308 & 334 & 246 & 056 & 000 & 026 & 000 \\ 419 & 316 & 346 & 246 & 059 & -44 & 014 & 000 \\ 334 & 303 & 315 & 272 & 026 & -31 & -33 & -0.5 \\ 264 & 259 & 334 & 352 & -08 & -13 & -76 & 43.5 \\ 228 & 259 & 272 & 346 & 018 & -39 & -15.5 & 73.5 \\ 246 & 246 & 259 & 290 & -26 & 000 & -28.5 & 77.5 \end{bmatrix}$$

- Thực hiện DWT đảo theo chiều ngang

$$\begin{bmatrix} 154 & 123 & 123 & 123 & 123 & 123 & 123 & 136 \\ 192 & 180 & 136 & 154 & 154 & 154 & 136 & 110 \\ 254 & 198 & 154 & 154 & 180 & 154 & 123 & 123 \\ 239 & 180 & 136 & 180 & 180 & 166 & 123 & 123 \\ 180 & 154 & 136 & 167 & 141 & 174 & 136 & 136 \\ 128 & 136 & 123 & 136 & 129 & 205 & 198 & 154 \\ 123 & 105 & 110 & 149 & 128 & 144 & 210 & 136 \\ 110 & 136 & 123 & 123 & 115 & 144 & 184 & 106 \end{bmatrix}$$

Ảnh *I*’ chứa tin giấu được tạo với ma trận điểm ảnh như trên.

c) Quy trình tách tin

Hình 2.7 mô tả chi tiết quá trình tách tin trong ảnh sử dụng kỹ thuật DWT. Từ sơ đồ tách tin được mô tả trong hình 2.7 có thể thấy được các bước chính của quá trình tách tin trong kỹ thuật biến đổi DWT như sau [15]:

- Thực hiện biến đổi DWT chia ảnh chứa tin *I’* thành 4 ảnh phụ I'_A, I'_H, I'_V, I'_D.

- Chia các ảnh I'_A, I'_H, I'_V, I'_D thành các khối 4x4 điểm ảnh (thực hiện quá trình Blocking) $B_{I'Ai}, B_{I'Hk}, B_{I'Vl}, B_{I'Dp}$ tương ứng.

- Lấy các khối phù hợp nhất $B_{I'Ai}$ từ ảnh phụ I'_A sử dụng khóa K_1.

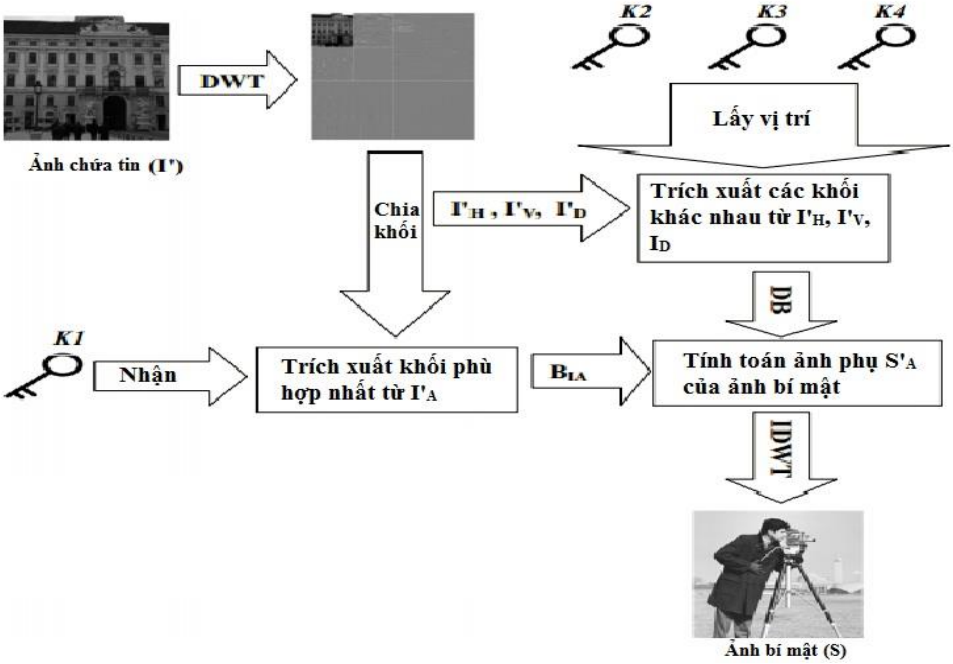
- Lấy các khối chênh lệch DB_i từ các ảnh phụ I'_H, I'_V, I'_D sử dụng khóa K_2, K_3, K_4 tương ứng.

- Tính toán khối bí mật B_{SA} qua công thức 2.21 như sau:

$$B_{SAi} = B_{IA'j} - DB'_i, \forall i = 1, \ldots, S_{An} \text{ và } j = 1, \ldots, I'_{An} \quad (2.21)$$

- Sử dụng khóa K_1 để sắp xếp lại thứ tự của các khối bí mật nhằm khôi phục ảnh phụ chứa hệ số xấp xỉ của ảnh bí mật S'_A

- Phân bổ các ảnh phụ S'_H, S'_V, S'_D là không, sau đó thực hiện DWT ngược trên cả S'_H, S'_V, S'_D và S'_A để thu được ảnh bí mật được giấu.



Hình 2.7. Mô hình tách tin trong kỹ thuật DWT

d) Nhận xét về phương pháp

Phương pháp giấu tin trong ảnh sử dụng DWT là một trong những phương pháp phổ biến và hiệu quả để giấu tin trong ảnh. Nó cho phép giấu tin một cách bí mật, vì thông tin được giấu vào các giá trị tần số của ảnh và không dễ dàng phát hiện được bởi mắt thường. Ngoài ra, do thông tin giấu được phân bố đồng đều trên toàn bộ ảnh nên rất khó phát hiện cũng như không làm thay đổi kích thước ảnh. Tuy nhiên, phương pháp này cũng có một số nhược điểm nhất định như sau. Thứ nhất để giấu tin một cách hiệu quả và an toàn, việc chọn các tham số như kích thước khối, giá trị ngưỡng là rất quan trọng. Nếu các tham số này được chọn một cách không thích hợp, thông tin giấu tin có thể bị mất hoặc dễ bị phát hiện. Do đó, nó cần được sử dụng với cẩn thận và các chi tiết cần được xem xét kỹ trước khi thực hiện phương pháp này. Tiếp theo, quá trình giấu tin và tách tin tương đối phức tạp, tốn thời gian.

2.4. Tổng kết chương 2

Trong chương 2, giáo trình đã trình bày một số vấn đề liên quan đến giấu tin trong ảnh bao gồm: Khái niệm, các định dạng ảnh.... Bên cạnh đó, trong chương này giáo trình đã trình bày một số phương pháp giấu tin trong ảnh phổ biến dựa trên các miền không gian và miền tần số của ảnh. Các phương pháp giấu tin trên miền không gian thường tìm cách thay thế các bit của thông tin cần giấu vào các bit của điểm ảnh. Còn các kỹ thuật giấu tin trong

ảnh dựa trên miền tần số thường giấu được nhiều thông tin, khả năng phát hiện ra các điểm bất thường trong ảnh khó hơn [16]. Do những ưu điểm vượt trội của các phương pháp này nên kỹ thuật giấu tin trong ảnh dựa trên miền tần số được ứng dụng rộng rãi ngày nay. Phương pháp này có thể được áp dụng trong cả 2 lĩnh vực của giấu tin là giấu tin mật và thủy vân số [1]. Trong thực tế, ngoài một số kỹ thuật giấu tin trong ảnh đã được trình bày trong giáo trình thì còn rất nhiều những kỹ thuật giấu tin khác. Ví dụ, trong tài liệu [1] đã liệt kê một số phương pháp giấu tin dựa trên miền không gian bao gồm: phương pháp giấu khối; phương pháp Brundox; phương pháp Darmstadter-Dellegle-Quisquotter-McCa. Đối với kỹ thuật giấu tin trên miền tần số ảnh cũng có một số hướng tiếp cận khác như [1]: Biến đổi Fourier rời rạc, phương pháp Koch và Zhao; Phương pháp Hsu và Wu....Ngoài những thuật toán trên, trong tài liệu [36] cũng đã liệt kê cách thức cài đặt một số phương pháp giấu tin trong ảnh bằng một số ngôn ngữ lập trình phổ biến.

2.5. Câu hỏi ôn tập và thực hành

Câu 1. Hãy trình bày về khái niệm giấu tin trong ảnh? Hãy phân tích các yêu cầu với kỹ thuật giấu tin trong ảnh?

Câu 2. Hãy trình bày các tiêu chí để phân loại giấu tin trong ảnh? Hãy liệt kê các thuật toán giấu tin trong ảnh theo các tiêu chí vừa nêu?

Câu 3. Hãy trình bày quy trình giấu tin và tách tin của kỹ thuật giấu tin LSB cổ điển?

Câu 4. Hãy trình bày quy trình giấu tin và tách tin của kỹ thuật giấu tin LSB nâng cao?

Câu 5. Hãy lấy ví dụ minh họa cho quá trình giấu tin và tách tin của kỹ thuật giấu tin LSB cổ điển?

Câu 6. Hãy lấy ví dụ minh họa cho quá trình giấu tin và tách tin của kỹ thuật giấu tin LSB nâng cao?

Câu 7. Hãy vẽ sơ đồ minh họa quá trình giấu tin và tách tin trong ảnh sử dụng kỹ thuật biến đổi DCT?

Câu 8. Hãy lấy ví dụ về quy trình giấu tin sử dụng kỹ thuật DCT? Hãy lấy ví dụ minh họa?

Câu 9. Hãy trình lấy ví dụ về quy trình tách tin sử dụng kỹ thuật DCT? Hãy lấy ví dụ minh họa?

Câu 10. Hãy trình bày về một ứng dụng của kỹ thuật giấu tin trong ảnh? Hãy nêu rõ kỹ thuật giấu tin và tách tin được sử dụng trong ứng dụng?

Câu 11. Liệt kê và phân tích ưu điểm và nhược điểm của các kỹ thuật giấu tin trong ảnh dựa sử dụng kỹ thuật biến đổi DCT và DWT.

Câu 12. Hãy phân tích và đánh giá ưu điểm, nhược điểm của 3 kỹ thuật giấu tin trong ảnh phổ biến LSB, DCT, DWT.

Câu 13. Cho tin cần giấu: “Các kỹ thuật giấu tin” và một ảnh bất kỳ (tự chọn). Bằng ngôn ngữ lập trình hãy thực hiện các yêu cầu sau:

a) Biến đổi tin cần giấu về dạng nhị phân.
b) Giấu tin cần giấu vào 2 bit LSB của ảnh.
c) Tính toán sự khác biệt giữa ảnh ban đầu và ảnh sau khi đã được giấu tin thông qua ma trận điểm ảnh.

Câu 14. Cho tin cần giấu: "Các kỹ thuật giấu tin" và một ảnh bất kỳ (tự chọn). Bằng ngôn ngữ lập trình hãy thực hiện các yêu cầu sau:

a) So sánh và đánh giá ảnh ban đầu và ảnh đã được xử lý bằng phương pháp DCT thông qua ma trận điểm ảnh.
b) Giấu tin vào ảnh sử dụng hệ số DC.
c) Giấu tin vào trong ảnh sử dụng hệ số AC.
d) So sánh và đánh giá ảnh giấu tin vào hệ số AC với ảnh giấu tin vào hệ số DC thông qua ma trận điểm ảnh.

Câu 15. Cho tin cần giấu: "Các kỹ thuật giấu tin" và một ảnh bất kỳ (tự chọn). Bằng ngôn ngữ lập trình hãy thực hiện các yêu cầu sau:

a) So sánh và đánh giá ảnh ban đầu và ảnh đã được xử lý bằng phương pháp DWT.
b) Giấu tin vào ảnh bằng phương pháp DWT kết hợp LSB
c) So sánh và đánh giá ảnh ban đầu với ảnh đã được giấu tin thông qua thông qua ma trận điểm ảnh.

Câu 16. Cho tin cần giấu: "Các kỹ thuật giấu tin" và một ảnh bất kỳ (tự chọn). Bằng ngôn ngữ lập trình hãy thực hiện giấu tin tin vào ảnh bằng các phương pháp LSB, DCT, DWT sau đó tiến hành thử nghiệm sau.

a) Thực hiện kỹ thuật nén ảnh sau đó tiến hành trích xuất thông tin giấu trong ảnh. Nhận xét và đánh giá về kết quả đạt được của từng phương pháp giấu tin.
b) Thực hiện kỹ thuật xoay ảnh sau đó tiến hành trích xuất thông tin giấu trong ảnh. Nhận xét và đánh giá về kết quả đạt được của từng phương pháp giấu tin.

Câu 17. Tìm hiểu về ứng dụng của giấu tin trong ảnh y tế. Hãy thực hiện giấu các thông tin về bệnh nhân và bác sỹ vào ảnh y tế?

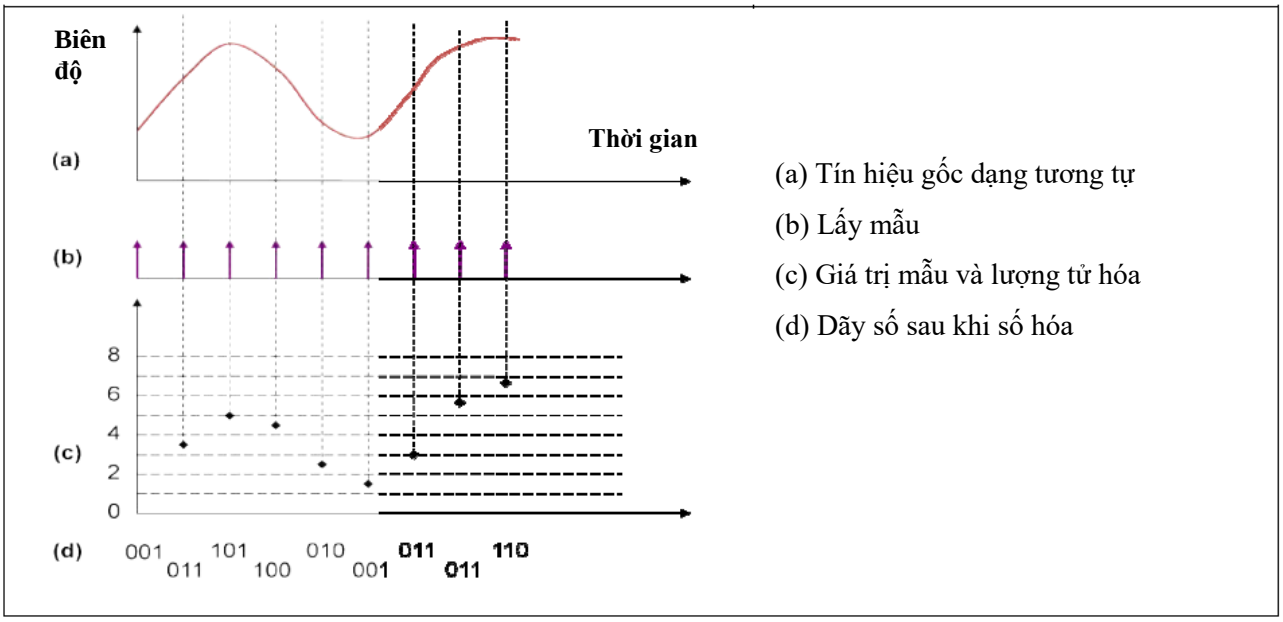
Câu 18. Thực hành tấn công lên các phương pháp giấu tin trong ảnh sử dụng công cụ VSCode?

CHƯƠNG 3: GIẤU TIN TRONG ÂM THANH

3.1. Tổng quan về giấu tin trong âm thanh

3.1.1. Đặc điểm của kỹ thuật giấu tin trong âm thanh

Trong phần 1.2 giáo trình đã trình bày khái niệm về giấu tin trong âm thanh. Theo đó, các vật chứa được sử dụng để giấu tin là các file âm thanh với các chuẩn khác nhau. Các vật chứa này sẽ bao gồm các đặc trưng như tần số, bước sóng, chu kỳ và biên độ, vận tốc lan truyền (tốc độ âm thanh)... Các kỹ thuật giấu tin sẽ tìm cách giấu tin vào âm thanh thông qua các khe hở như tần số, biên độ, chu kỳ,… Hình 3.1 trình bày ví dụ về một tín hiệu âm thanh và mẫu.



Hình 3.1. Ví dụ về tín hiệu âm thanh và mẫu

Từ hình 3.1 thấy được một số đặc điểm cần lưu ý trong kỹ thuật giấu tin trong âm thanh bao gồm:

- Tần số mẫu: Để đưa được âm thanh vào các ứng dụng của giấu tin, cần xác định biên độ dao động của sóng âm vào các thời điểm khác nhau. Công việc này gọi là trích/lấy mẫu. Cụ thể, với một giây phát ra âm thanh, người dùng sẽ trích lấy mẫu biên độ và đưa vào dữ liệu, con số ấy gọi là tần số lấy mẫu (sample rate). Tần số này cho biết biên độ rung mỗi giây của sóng âm thanh. Ví dụ, tần số mẫu là 44,1 kHz thì mỗi giây tín hiệu nhận được bị cắt thành 44100 lát.

- Độ sâu của bit: Để lưu lại dưới dạng số, mỗi mẫu được biểu diễn bằng một lượng bit dữ liệu nhất định gọi là BitDepth. Ví dụ với một file âm thanh dạng WAV thường là 8 hoặc 16 bit. BitDepth càng lớn thì âm thanh lấy mẫu càng chính xác và người nghe càng thấy sắc

nét, rõ ràng. Giả sử, nếu lấy được mẫu với tần số 44,1kHz (44100 lần/giây), 16 bit (tương đương với chất lượng CD) thì khi đó 1 phút âm thanh sẽ chiếm 10MB ổ cứng.

- Kích thước mẫu trích: Công thức kích thước mẫu trích (được tính bằng byte) như sau: Kích thước mẫu = Kênh âm thanh x Tần số trích mẫu / 8.

- Âm thanh số: là các mẫu lấy theo phương pháp lượng tử hóa, chuyển đổi giá trị mẫu từ dạng liên tục thành các giá trị rời rạc.

3.1.2. Một số định dạng file âm thanh và công cụ xử lý âm thanh

a) Một số định dạng âm thanh cơ bản

Có thể phân loại định dạng file âm thanh thành một số định dạng chính như sau:

- WAV (.wav): là kiểu định dạng đại diện cho âm thanh kỹ thuật số trong hệ điều hành Windows.
- AIFF (.aif) và AU (.au): *AIFF* là kiểu định dạng âm thanh đại diện cho Macintosh, AU là kiểu định dạng đại diện cho hệ thống Sun.
- RealAudio (.ra): là hệ thống được sử dụng đầu tiên đại diện cho luồng âm thanh và hình ảnh trên Internet.
- MIDI (.mid): được ghi tắt của Music Instrument Digital Interface, là chuẩn đại diện cho thông tin âm nhạc chuyển giao giữa phương tiện điện tử và máy tính.
- QuickTime (.qt): được sử dụng để định dạng đa phương tiện từ máy tính Apple, hỗ trợ cả luồng âm thanh và luồng hình ảnh.

b) Một số công cụ xử lý âm thanh

Một số sản phẩm đã được phát triển và ứng dụng cho lĩnh vực giấu tin trong âm thanh như sau (xem bảng 3.1). Bảng 3.1 đã liệt kê một số sản phẩm mã nguồn mở và miễn phí. Dựa trên các sản phẩm và công cụ này người dùng có thể sử dụng để thực hiện quá xử lý các tập tin âm thanh rồi sử dụng các kỹ thuật giấu tin trong âm thanh để giấu tin vào chúng [1].

Bảng 3.1. Một số phần mềm hỗ trợ giấu tin trong âm thanh

Tên phần mềm giấu	**Định dạng file âm thanh**
Info Stego	mp3
ScramDisk	wav
MP3Stego	mp3
StegoWav	wav
Hide4PGP	mp3, voc
Invisible Secrets	wav

[1] Mô tả về một số công cụ: http://lib.uet.vnu.edu.vn/bitstream/123456789/979/1/Luan_an_Huynh_Ba_Dieu.pdf

Tên phần mềm giấu	Định dạng file âm thanh
Steganos	wav, voc

3.1.3. Phân loại phương pháp giấu tin trong âm thanh

Trong tài liệu [1, 2] đã liệt kê một số kỹ thuật giấu tin trong âm thanh. Theo đó, các kỹ thuật giấu tin trong âm thanh có thể được phân loại thành hai loại chính như sau:

- Phân loại theo kỹ thuật giấu tin: Phương pháp phân loại theo kỹ thuật giấu tin dựa vào đặc tính và tính chất của kỹ thuật được sử dụng để giấu tin. Theo tiêu chí này, các kỹ thuật giấu tin trong âm thanh chia làm một số phương pháp như sau: Phương pháp LSB; Phương pháp trải phổ; Phương pháp mã hóa pha; Phương pháp tiếng vang; Phương pháp tự đánh dấu....

- Phân loại theo đặc điểm tín hiệu gốc: Đối với cách phân loại này, các phương pháp giấu tin trong âm thành được phân thành 2 loại chính:

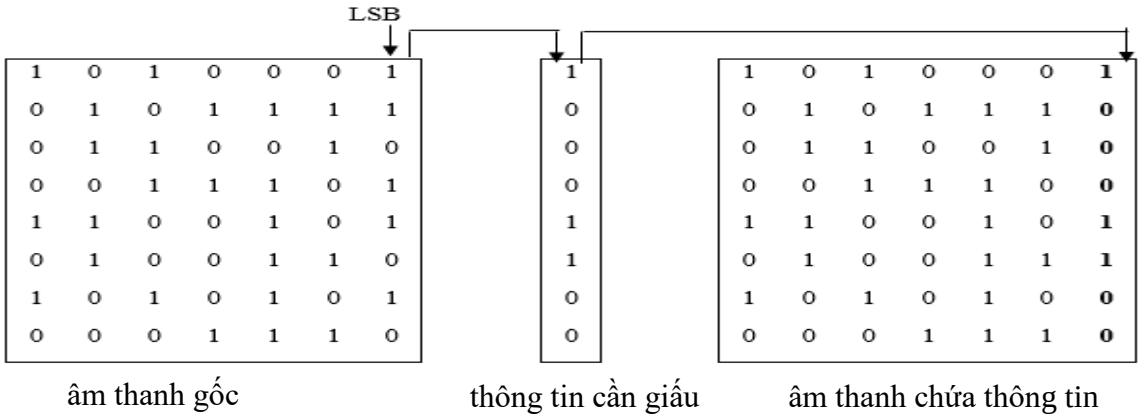
+ Giao thoa tín hiệu gốc: Các phương pháp thuộc nhóm này đều cần đến tín hiệu gốc khi muốn rút trích thông tin. Tuy nhiên, trong các ứng dụng thực tế nhóm phương pháp này lại tỏ ra không hiệu quả vì phải cần gấp đôi bộ nhớ để lưu trữ cùng một thông tin, cần đến gấp đôi lượng băng thông cho quá trình rút trích thông tin. Vì vậy, nhóm phương pháp này ít được nghiên cứu và phát triển. Phương pháp này thường được sử dụng trong việc chứng thực bản quyền. Một số thuật toán trong nhóm này như: Mã hóa pha; Điều chế pha.

+ Không giao thoa tín hiệu gốc: Các phương pháp thuộc nhóm này khi muốn trích xuất thông tin được giấu trong âm thanh thì không cần đến tín hiệu gốc hay bất kỳ thông tin nào khác (trừ khóa mật nếu có). Nhóm các phương pháp này chỉ cần đến một nửa bộ nhớ lưu trữ và một nửa băng thông để rút trích so với nhóm phương pháp cần tín hiệu gốc. Một số thuật toán trong nhóm này như: Các phương pháp trải phổ; Các phương pháp tập đôi; Các phương pháp sử dụng bản sao; Các phương pháp tự đánh dấu.

Trên đây giáo trình đã liệt kê về một số thuật toán và phương pháp, kỹ thuật giấu tin trong âm thanh khác nhau. Tiếp theo, giáo trình sẽ đi vào mô tả chi tiết về cách thức tiến hành giấu tin cũng như tách tin của một số kỹ thuật giấu tin trong âm thanh phổ biến. Ngoài ra, một số thuật toán khác không được mô tả trong giáo trình, người đọc có thể tham khảo thêm tại tài liệu [1, 2].

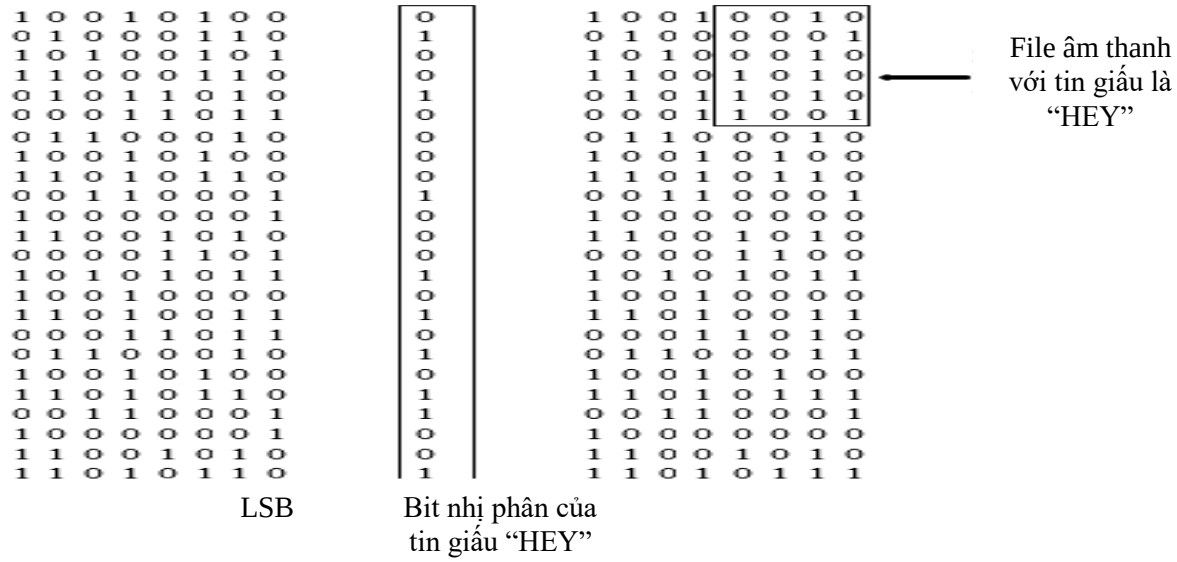
3.2. Phương pháp LSB

Cách thay thế LSB là cách đơn giản để giấu thông tin vào dữ liệu âm thanh kỹ thuật số. Chi tiết về phương pháp thay thế LSB đã được trình bày trong chương 2 (kỹ thuật giấu tin trong ảnh). Hình 3.2 thể hiện một ví dụ về phương pháp thay thế LSB với trường hợp thay thế 1 bit LSB [17].

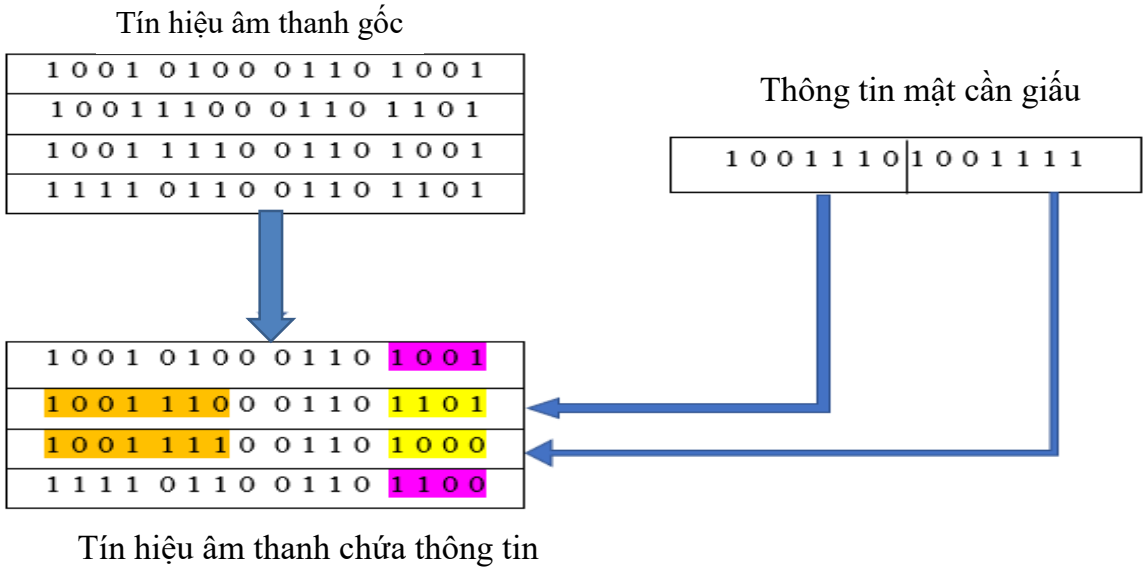


Hình 3.2. Mô tả phương pháp thay thế bit trong thuật toán LSB

Từ hình 3.2 có thể thấy, các kỹ thuật thay thế LSB trong âm thanh cũng được thực hiện giống như thực hiện trên ảnh. Theo đó, trước tiên cần chia dữ liệu âm thanh gốc thành các đoạn. Thông thường, người giấu tin sẽ chia dữ liệu âm thanh thành các đoạn dựa trên độ dài bit của thông tin cần giấu. Sau đó các đoạn này được biến đổi thành vector giá trị của tín hiệu, rồi lưu vào mảng một chiều. Đối với thông tin cần giấu (L), chúng cũng được biến đổi nhị phân rồi tính chiều dài chuỗi bit L cần giấu. Tiếp theo, người giấu tin sẽ chọn k là số bit LSB của tín hiệu âm thanh sẽ giấu sao cho phù hợp nhất. Cuối cùng, chia chuỗi bit thông điệp thành các chuỗi con có độ dài k bit. Trong đó, mỗi chuỗi con này sẽ được thay thế vào k bit LSB của L/k tín hiệu âm thanh để giấu đủ L bit thông điệp. Nhìn chung, phương pháp giấu tin trong âm thanh dựa trên thay thế LSB sẽ cho phép giấu được một lượng thông tin lớn và tốc độ truyền dữ liệu nhanh. Tuy nhiên, phương pháp này tương đối đơn giản nên dễ bị phát hiện. Để tăng độ an toàn cho kỹ thuật này, có thể sử dụng bộ sinh số ngẫu nhiên để sinh ra các vị trí các mẫu được chọn giấu thay vì chọn các mẫu liên tục. Bộ sinh số này sử dụng một khóa bí mật như là phần tử khởi tạo bộ sinh số. Khóa được sử dụng trong cả quá trình giấu tin và tách tin. Ngoài cách tiếp cận truyền thống như trên, hiện nay cũng có một số hướng tiếp cận khác nhằm nâng cao chất lượng giấu tin trong kỹ thuật LSB. Ví dụ phương pháp sử dụng 4 bit LSB thay vì 1 bit LSB đơn lẻ hoặc phương pháp kết hợp giữa bít quan trọng nhất (MSB -Most Significant Bit) và LSB. Chi tiết các phương pháp này đã được trình bày trong một số bài báo [16, 17]. Hình 3.3 và 3.4 mô tả quy trình giấu tin sử dụng 4 bit LSB và 7 bit MSB.



Hình 3.3. Giấu tin sử dụng 4 bit LSB



Hình 3.4. Kỹ thuật giấu tin trong âm thanh dựa vào 7 bit MSB và 4 bit LSB

3.3. Phương pháp mã hóa pha

3.3.1. Khái niệm về phương pháp mã hóa pha

Mã hóa pha là một phương pháp dựa vào đặc tính tai người không phân biệt được sự khác nhau về pha của hai tín hiệu âm thanh. Việc giấu tin được thực hiện thông qua việc thay thế một đoạn âm thanh ban đầu bằng một pha tham chiếu (referency phase) thể hiện dữ liệu. Pha của các đoạn tiếp theo sẽ được điều chỉnh sao cho độ chênh lệch pha giữa các đoạn là không đổi [14, 18]. Để hiểu rõ hơn về vấn đề này, hãy xem xét ví dụ sau đây: Giả sử có hai chuỗi *x(t)* và *y*(t) như sau:

$$x(t) = Acos\ (2\pi ft + \varphi)$$

$$y(t) = Asin(2\pi ft + \varphi) = Acos\ (2\pi ft + \varphi - \pi/2)$$

Trong đó:

A là biên độ, *f* là tần số và φ là pha.

Thuật ngữ pha được hiểu theo nghĩa đó là tham chiếu đến một tín hiệu nào khác. Ví dụ nếu tham chiếu đến tín hiệu *A*cos $(2\pi ft)$ thì tín hiệu *x(t)* có pha là φ và tín hiệu *y(t)* có pha là $\varphi - \pi/2$. Trong mã hóa pha, mỗi dữ liệu được coi là một dịch pha (phase shift) trong phổ pha của tín hiệu sóng mang. Xét tín hiệu sóng mang *c*, *c* được chia thành *N* phần nhỏ và mỗi phần tử $c_i(n)$ có chiều dài l_m (xem hình 3.5). Lúc này áp dụng biến đổi Fourier có:

+ Độ lớn tín hiệu được tính bằng công thức 3.1:

$$A_i(k) = \sqrt{R_e[F\{c_i\}(k)]^2 + l_m\left[F\{c_j\}(k)\right]^2} \quad (3.1)$$

+ Ma trận độ lớn pha có các phần tử được tính theo công thức 3.2 như sau:

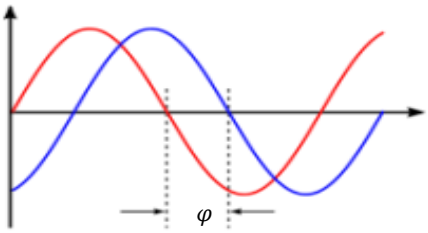
$$\varphi_i(k) = \arctan\frac{l_m[F\{c_i\}(k)]}{R_e[F\{c_i\}(k)]} \quad (3.2)$$

Trong đó:

R_e Là phần thực

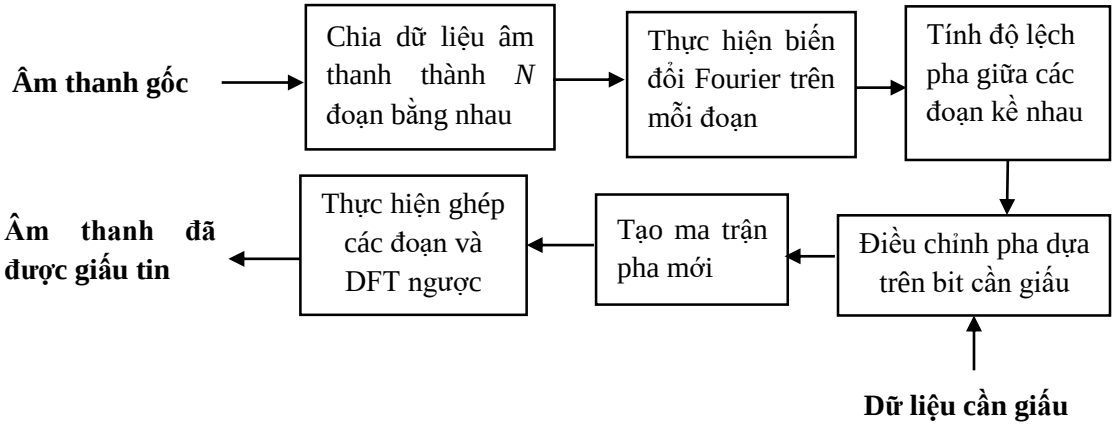
l_m Là phần ảo

i: là thời gian



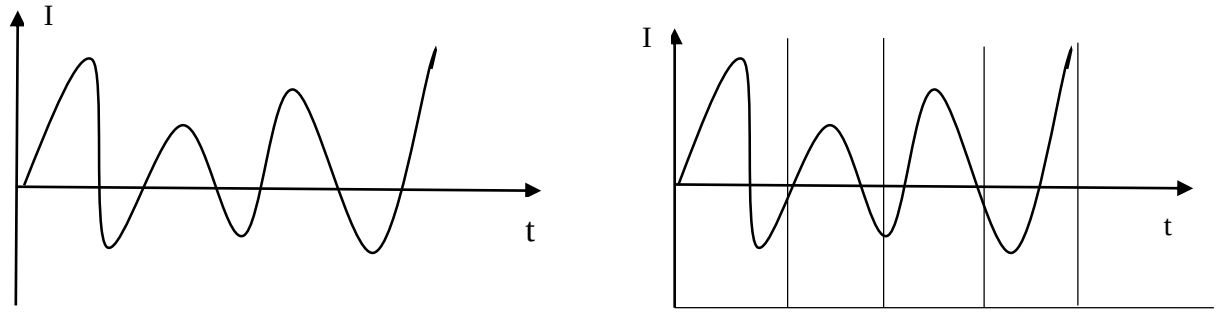
Hình 3.5. Ví dụ về sự dịch chuyển pha của tín hiệu

3.3.2. Quy trình giấu tin



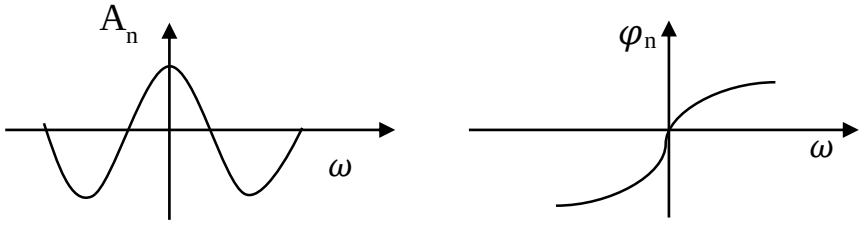
Hình 3.6. Quy trình giấu tin trong video bằng phương pháp mã hóa pha

Bước 1: Dữ liệu âm thanh gốc có chiều dài *N* được chia thành các đoạn có chiều dài bằng chiều dài với thông tin cần giấu. Hình 3.7 thể hiện ví dụ về một đoạn được tách từ âm thanh ban đầu.



Hình 3.7. Ví dụ chia âm thanh gốc thành các đoạn bằng nhau

Bước 2: Mỗi đoạn được biến đổi bằng Fourier DFT với ma trận độ lớn phase là $\varphi_j[\omega_k]$ và ma trận độ lớn tín hiệu là $A_j[\omega_k]$ với $0 \le k \le \frac{N}{2} - 1; 0 \le j \le N - 1$



Hình 3.8. Ví dụ về mỗi đoạn được biến đổi bằng DFT

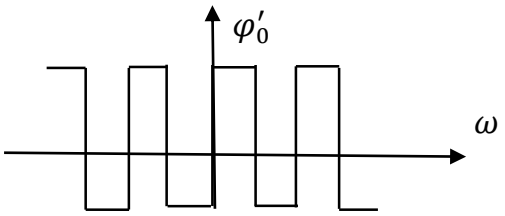
Bước 3: Tính độ lệch pha giữa các đoạn kề nhau. Việc tính toán này sẽ đảm bảo sự khác biệt giữa các pha sẽ không quá lớn sau khi tiến hành biến đổi. Quá trình tính độ lệch pha được thực hiện bằng công thức 3.3:

$$\Delta\varphi_j[\omega_k] = \varphi_{j+1}[\omega_k] - \varphi_j[\omega_k];\ \forall j,k \tag{3.3}$$

Bước 4: Điều chỉnh pha. Giá trị chính xác các pha của các đoạn có thể thay đổi nhưng mối liên hệ về sự khác nhau giữa các đoạn liên tiếp phải được đảm bảo. Việc điều chỉnh pha của đoạn đầu được áp dụng dựa trên công thức 3.4 như sau:

$$Phase\_new = \begin{cases} \frac{\pi}{2} & \text{nếu bit cần giấu } = 0 \\ -\frac{\pi}{2} & \text{nếu bit cần giấu } = 1 \end{cases} \tag{3.4}$$

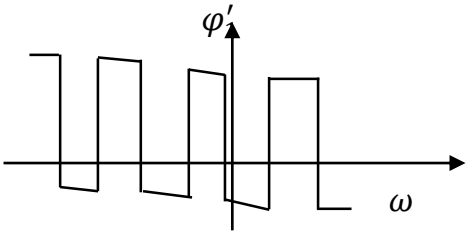
Khi đó thông tin giấu chỉ được phép giấu trong vector pha của đoạn đầu tiên (xem hình 3.9).



Hình 3.9. Tín hiệu được giấu trong pha của đoạn đầu tiên

Bước 5: Tiến hành tạo ma trận pha mới thỏa mãn để căn chỉnh lại độ chênh lệch tính ra ở bước 3. Tạo ma trận pha mới thỏa mãn điều kiện:

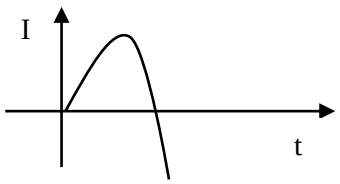
$$\varphi'_{j+1}[\omega_k] = \varphi'_j[\omega_k] + \Delta\varphi_{j+1}[\omega_k];\ \forall j,k$$



Hình 3.10. Ma trận pha mới được tạo

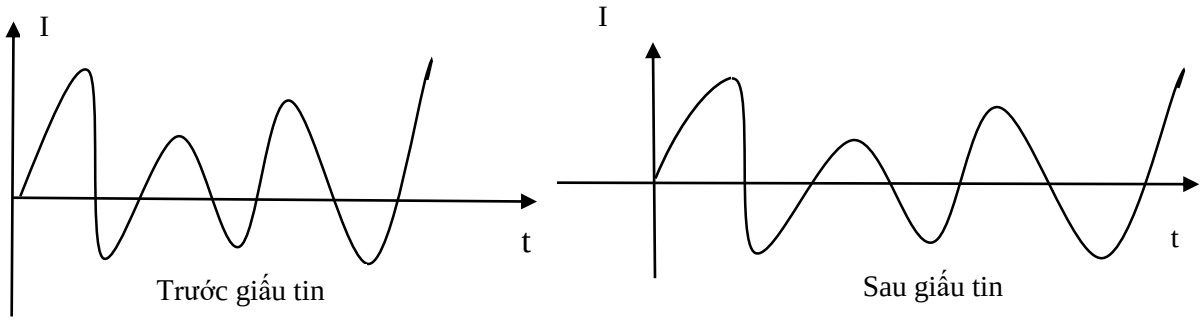
Trong thực tế luôn tìm được cặp $\varphi'_{j+1}[\omega_k]$ và $\varphi'_j[\omega_k]$ thỏa mãn công thức do Fourier rời rạc có tính đầy đủ (với mọi $N>0$, mọi vectơ phức N chiều đều có một DFT và một IDFT đồng thời DFT và IDFT đều là các vectơ phức nhiều chiều). So sánh hình 3.9 và hình 3.10 thấy được rằng ma trận pha mới tạo đã có sự thay đổi so với ma trận pha ban đầu.

Bước 6: Kết hợp với cường độ pha của tín hiệu cũ sau khi đã giấu thông tin. Mục đích của bước này chính là tái tạo lại ma trận pha của các đoạn kề nhau (xem hình 3.11). Pha mới bằng pha kề trước đó cộng với độ lệch pha đã được tính ở trên.



Hình 3.11. Pha mới được tạo ra sau khi kết hợp cường độ của pha cũ

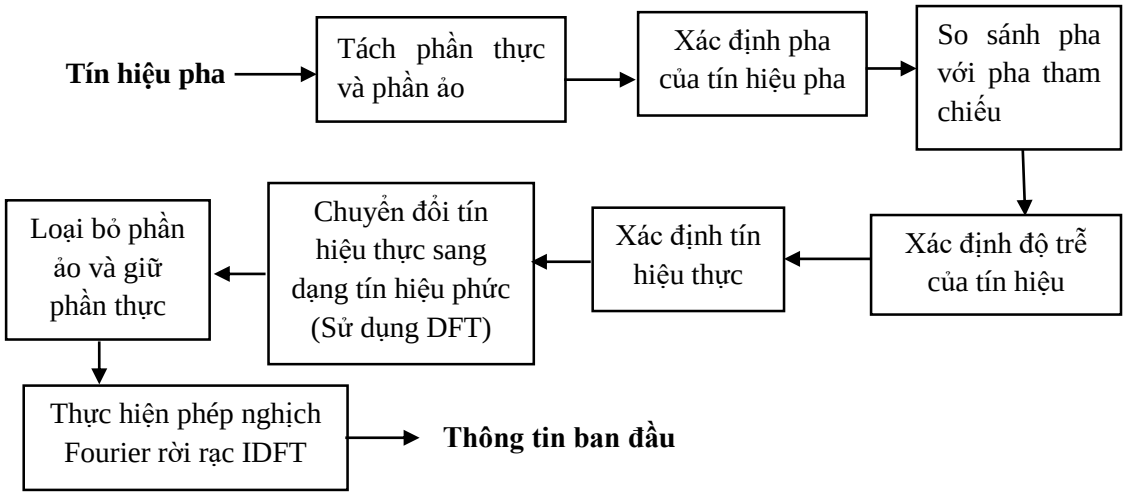
Bước 7: Thực hiện ghép các đoạn lại và DFT ngược để tạo lại dữ liệu âm thanh. Để nhận được tin giấu bằng kỹ thuật này, người nhận phải biết độ dài của đoạn, sau đó thực hiện DFT để nhận tin.



Hình 3.12. So sánh pha trước và sau khi giấu tin

Từ hình 3.12 dễ dàng nhận thấy rằng âm thanh đã bị thay đổi về cấu trúc pha khi sau giấu thông tin.

3.3.3. Quy trình tách tin



Hình 3.13. Quy trình tách tin

Quy trình tách tin trong âm thanh được thực hiện theo sơ đồ hình 3.13 như sau: Trước tiên tín hiệu pha được truyền đến bộ giải mã. Bộ giải mã tách phần thực và phần ảo của tín hiệu pha bằng cách sử dụng phép toán số phức. Phần thực và phần ảo của một tín hiệu phức

hợp được sử dụng để đại diện cho thông tin về biên độ và pha của tín hiệu đó. Phần thực và phần ảo được xác định bằng cách sử dụng phép biến đổi Fourier hoặc phép biến đổi ngược Fourier. Khi tín hiệu phức hợp được biểu diễn dưới dạng phần thực và phần ảo thì người dùng có thể phân tích và tái tạo lại tín hiệu ban đầu. Để tách phần thực và phần ảo của tín hiệu pha, có thể sử dụng các phép toán số phức như cộng, trừ, nhân, chia. Trong tài liệu [14] đã trình bày chi tiết quá trình tách phần thực và phần ảo này. Tiếp theo cần xác định pha của tín hiệu pha: Pha của tín hiệu pha được xác định dựa trên phương pháp so sánh pha. Theo đó, phương pháp này dựa trên việc so sánh pha của tín hiệu cần đo với pha của tín hiệu tham chiếu. Nếu chúng có cùng pha, thì độ trễ pha sẽ bằng 0. Nếu chúng không đồng pha, lúc này có thể tính độ trễ pha bằng cách sử dụng các công thức toán học [14, 18]. Cũng có thể sử dụng phương pháp xử lý tín hiệu để xác định pha của tín hiệu. Các kỹ thuật này có thể bao gồm biến đổi Fourier, biến đổi Laplace... Tiếp theo, xác định độ trễ của tín hiệu bằng cách so sánh pha với pha tham chiếu. Trong đó, pha tham chiếu là pha của một tín hiệu được coi là tín hiệu chuẩn. Pha tham chiếu thường được chọn là pha của tín hiệu có tần số cao hơn và được coi là tín hiệu chính. Pha của các tín hiệu khác được so sánh với pha tham chiếu để xác định độ trễ của chúng. Sau đó, xác định tín hiệu thực dựa trên sự khác biệt giữa pha của tín hiệu pha và pha của tín hiệu tham chiếu. Cuối cùng là tái tạo lại tín hiệu thực. Để thực hiện được mục tiêu này người tách tin sẽ chuyển đổi tín hiệu thực sang dạng tín hiệu phức bằng phép biến đổi DFT, rồi loại bỏ phần ảo và giữ lại phần thực của các giá trị phức. Sau đó là thực hiện DFT nghịch trên các giá trị phức phần thực vừa được lấy ra để tái tạo tín hiệu thực. Kết thúc giai đoạn này người giấu tin sẽ thu được tín hiệu cần tìm.

3.3.4. Nhận xét về phương pháp

- Ưu điểm:
  + Khó phát hiện: như đã trình bày ở trên mã hóa pha với thay đổi đủ nhỏ sẽ không bị phát hiện bởi giác quan của con người do hệ thính giác không nhạy cảm với sự thay đổi của pha âm thanh.
  + Không gây nhiễu như các phương pháp với LSB hoặc các phương pháp khác.
- Nhược điểm:
  + Lượng thông tin được giấu nhỏ vì phương pháp mã hóa pha chỉ giấu được thông tin trên một đoạn nhỏ của âm thanh. Nếu muốn tăng lượng thông tin được giấu thì có thể kéo dài thêm đoạn của âm thanh gốc, tuy vậy việc đó ít được thực hiện bởi nếu vậy khả năng bị phát hiện tin được giấu trong file âm thanh sẽ lớn hơn.
  + Khả năng ứng dụng bị hạn chế: Ví dụ nếu sử dụng mã hóa pha để giấu tin trong âm thanh, âm thanh đó có thể dễ dàng bị phát hiện và tấn công do thông tin cần giấu chỉ ở đầu của âm thanh.
  + Quá trình giấu tin và tách tin phức tạp, tốn thời gian.

Ngoài các kỹ thuật xử lý truyền thống để giấu tin bằng phương pháp mã hóa pha thì các nguyên cứu và đề xuất gần đây thường tập trung vào đề xuất một số kỹ thuật xử lý tiên

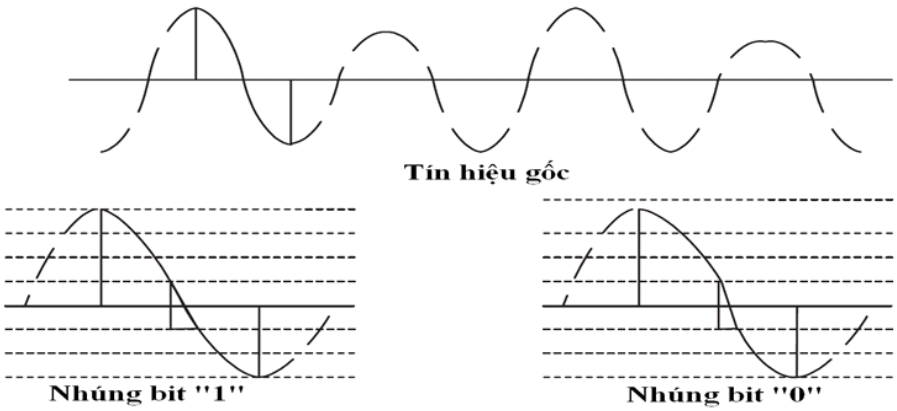
tiến nhằm giải quyết một số vấn đề gặp phải của mã hóa pha truyền thống [27]. Cụ thể, để tối ưu hóa về mặt thời gian, phương pháp mã hóa pha cải tiến [27] đã đề xuất sử dụng thuật toán Fast Fourier Transform (FFT), được phát triển bởi Cooley và Tukey vào khoảng năm 1965. Ý tưởng thuật toán này dựa vào trên việc khai triển biến đổi Fourier rời rạc của dãy có chiều dài $N = 2^x$ thành các tầng lớp nhỏ hơn. Điều kiện để sử dụng thuật toán này là N phải có dạng $N = 2^x$. Với hướng tiếp cận này, độ phức tạp của thuật toán là lúc này chỉ còn là $O(N \log N)$ thay vì $O(N^2)$ như mã hóa pha truyền thống. Chi tiết quá trình giấu tin và tách tin trong âm thanh dựa trên mã hóa pha cải tiến này được trình bày trong tài liệu [27].

3.4. Một số phương pháp khác

3.4.1. Phương pháp tự đánh dấu

Phương pháp tự đánh dấu là phương pháp mà thông tin được giấu vào bằng cách tự đặt các dấu hiệu dùng để xác minh vào trong tín hiệu của âm thanh. Phương pháp tự đánh giấu có thể được thực hiện bằng cách nhúng một tín hiệu đặc biệt vào trong âm thanh hoặc thay đổi hình dạng của tín hiệu trên miền thời gian hay miền tần số thông qua các kỹ thuật như điều chỉnh tỉ lệ thời gian và dựa vào đặc trưng quan trọng nhất. Tiếp theo, giáo trình sẽ đi vào mô tả chi tiết hai kỹ thuật này.

- Điều chỉnh tỉ lệ thời gian: Kỹ thuật giấu tin sử dụng phương pháp điều chỉnh tỉ lệ thời gian (Steganography using Time-Scale Modification -STSM) là một phương pháp giấu tin trong đó thông tin được giấu vào giữa các khoảng thời gian của tín hiệu âm thanh. Cụ thể, thông tin được giấu bằng cách thay đổi khoảng thời gian giữa các mẫu âm thanh. Trong tỉ lệ thời gian điều chỉnh, các mẫu âm thanh được chuyển đổi theo một mẫu được xác định trước, với khoảng thời gian giữa các mẫu được điều chỉnh để giấu thông tin. Việc điều chỉnh khoảng thời gian này có thể được thực hiện bằng cách tăng hoặc giảm khoảng cách giữa các mẫu trong một tập tin âm thanh. Ý tưởng thực hiện là thay đổi tỉ lệ thời gian giữa hai cực là cực đại và cực tiểu. Khoảng cách giữa hai cực được chia thành N phân đoạn có biên độ bằng nhau. Lúc này sẽ thay đổi độ dốc của tín hiệu, tùy thuộc vào bit muốn nhúng.



Hình 3.14. Quy tắc giấu thông tin sử dụng phương pháp điều chỉnh tỉ lệ thời gian

Hình 3.14 mô tả quy tắc giấu thông tin vào âm thanh dựa trên kỹ thuật điều chỉnh tỉ lệ thời gian. Từ hình 3.14 thấy rằng: tín hiệu âm thanh khi chứa giấu thông tin thì tín hiệu âm thanh dưới dạng sóng với những biên độ khác nhau do các giá trị cực đại, cực tiểu khác nhau. Nhưng biên độ giữa các phân đoạn *N* là như nhau và chỉ khác nhau ở giá trị cực đại và cực tiểu. Từ quy tắc nhúng bit 0 và bit 1 vào tín hiệu âm thanh bằng phương pháp điều chỉnh tỷ lệ thời gian dẫn đến đường tín hiệu đi từ giá trị cực đại đến cực tiểu sẽ bị thay đổi độ dốc. Với dữ liệu đầu vào là: Tệp âm thanh gốc *C*; Chuỗi bit *M* cần giấu có độ dài *L* (*L* là bội số của 8). Quy trình giấu thông tin trong tín hiệu âm thanh bằng phương pháp điều chỉnh tỉ lệ thời gian được tiến hành theo 2 bước như sau:

+ **Bước 1**: Mã hóa: Chuỗi bit *M* được chia thành các đoạn M_i có độ dài 4 bit. Mỗi đoạn bit thông tin này sẽ được mã hoá bằng phương pháp mã Hamming. Với phương pháp mã hóa Hamming thì các đoạn M_i được biến đổi từ 4 bit thành từ mã có độ dài 7 bit. Ghép các chuỗi bit kết quả lại để được chuỗi bit *M*'. Độ dài chuỗi *M*' sẽ bằng (*L/4*) x7.

+ **Bước 2**: Giấu tin: Trước tiên vật chứa *C* sẽ được xử lý để trích phần header và phần dữ liệu. Người giấu tin sẽ tiến hành kiểm tra vật chứa *C* có đủ để giấu chuỗi bit *M*' không. Nếu không đủ thì dừng và báo không giấu được. Nếu đủ thì sẽ ghi header của *C* vào *C*' sau đó thực hiện giấu từng bit của chuỗi *M*' vào phần dữ liệu của *C* để ghi ra C'. Sau quá trình kiểm tra thỏa mãn thì tiến hành trích tuần tự 3 mẫu dữ liệu của *C* và tính tổng:

  o Nếu bit đang xét của *M*' là 1 mà tổng lẻ thì thỏa mãn điều kiện giấu, không cần điều chỉnh. Nếu tổng chẵn thì điều chỉnh mẫu số 2 của 3 mẫu đang xét để cho tổng là số lẻ.

  o Nếu bit đang xét của *M*' là 0 mà tổng chẵn thì đã thỏa mãn điều kiện giấu, không cần điều chỉnh, ngược lại điều chỉnh mẫu 1 hoặc mẫu thứ 3 trong 3 mẫu đang xét để cho tổng là số chẵn.

  o Ghi 3 mẫu đang xét ra tệp *C*'. Lặp lại quá trình kiểm tra trên cho đến khi toàn bộ các bit của chuỗi *M*' đã được giấu.

Cuối cùng là công đoạn ghi các mẫu còn lại từ *C* vào *C*' và kết thúc. Nhìn chung, STSM là một phương pháp giấu tin hiệu quả và khó phát hiện, vì nó không làm thay đổi nội dung của tín hiệu âm thanh, mà chỉ thay đổi khoảng thời gian giữa các mẫu. Một ưu điểm của STSM là nó có thể được áp dụng cho nhiều loại tín hiệu âm thanh như: WAV, MP3, …

- **Dựa vào đặc trưng quan trọng nhất:** Đặc trưng quan trọng nhất chính là các tín hiệu đặc biệt và gây được sự chú ý. Phương pháp này còn được gọi là phương pháp mã hóa dựa trên khoa học tâm sinh lý nghe (Psychoacoustics) – Cách thức con người cảm nhận âm thanh. Đặc tính chính của phương pháp cảm nhận này là một số âm thanh đặc biệt có thể che được các âm thanh khác. Vì vậy để giấu tin chỉ cần tần số bằng tần số của âm thanh đặc biệt vì khi đó người nghe không thể nghe được âm thanh bị che đi. Đây gọi là che tần số. Che tần số là khả năng một âm thanh lớn trong một băng tần sẽ che những âm thanh có tần số thấp hơn. Do đó người nghe chỉ có thể cảm nhận được những âm thanh có tần số lớn hơn.

Quá trình giấu tin và tách tin trong âm thanh dựa vào đặc trưng quan trọng nhất được thực hiện theo các bước như sau: Trước tiên, cần chia dữ liệu âm thanh thành các đoạn S_i có cùng kích thước n. Tiếp theo sẽ thực hiện giấu thông tin trong từng bit trên mỗi đoạn S_i. Quy tắc giấu bit 0 và bit 1 được thực hiện theo công thức điều chỉnh để giấu:

$$S_i'(n) = \begin{cases} 0.99 \times S_i(n) & \text{cho bit 1} \\ 0.98 \times S_i(n) + S_i(n-d) & \text{cho bit 0} \end{cases} \quad (3.5)$$

Có thể thấy rằng: phương pháp giấu tin trong âm thanh dựa trên đặc trưng quan trọng nhất có ưu điểm là đảm bảo tính bí mật và khó bị phát hiện do chúng không làm thay đổi chất lượng tín hiệu âm thanh gốc. Bên cạnh đó, sử dụng phương pháp này thì người dùng có thể giấu được nhiều thông tin hơn so với các phương pháp khác. Mặc dù vậy, nhược điểm của này là khó khăn trong việc tìm kiếm các đặc trưng quan trọng nhất phù hợp để đánh dấu thông tin. Ngoài ra, quá trình trích xuất thông tin của phương pháp cũng gặp nhiều khó khăn, chỉ cần thay đổi nhỏ cũng có thể dẫn đến các thông tin trích xuất bị sai lệch.

3.4.2. Phương pháp trải phổ

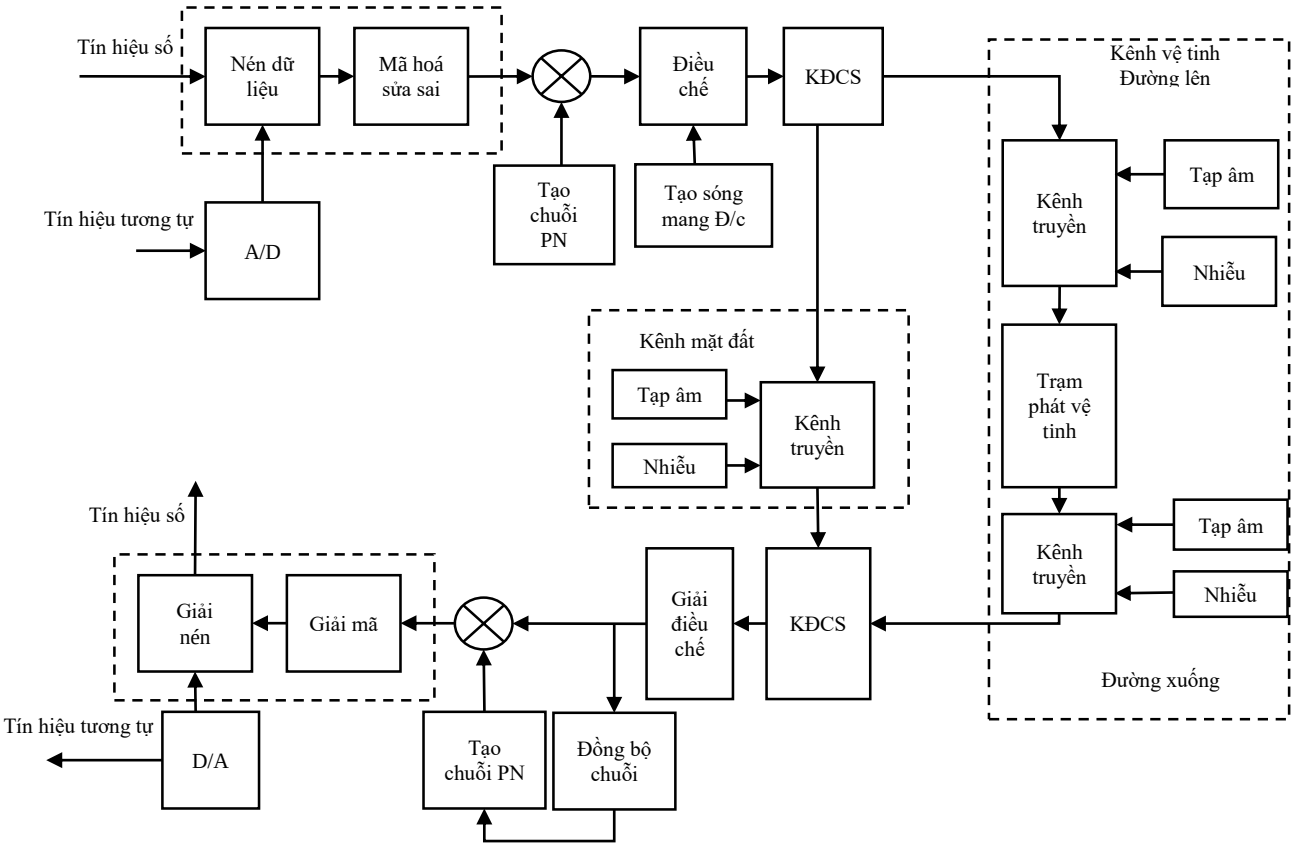
a) Giới thiệu chung

Trải phổ là kỹ thuật truyền tín hiệu được sử dụng rộng rãi trong truyền thông. Trong đó năng lượng của tín hiệu được "trải" trên một băng thông rộng hơn nhiều lần so với lượng băng thông cần thiết nhờ sử dụng mã giả ngẫu nhiên độc lập với tín hiệu thông tin. Tín hiệu trải phổ trông giống như nhiễu, khó phát hiện và thậm chí khó để chặn đứng hay giải điều chế (demodulation) nếu không có các thiết bị thích hợp. Do lợi ích của trải phổ là làm cho tín hiệu khó bị phát hiện cùng với đó là cách tiến hành giống như việc trải thông tin mật lên toàn bộ phương tiện chứa nên các nhà nghiên cứu đã áp dụng kỹ thuật này để giấu tin trong âm thanh. Quy trình thực hiện trải phổ có thể hiểu một cách tổng quát như sau [18 - 23]:

- Máy phát là *A* muốn truyền thông tin mật *M* đến máy phát *B* thì sẽ tiến hành chia thông tin *M* thành *n* gói thông tin nhỏ $\{s_1, s_2, \ldots, s_n\}$. Trước khi đưa lên kênh truyền dẫn mỗi gói tin nhỏ s_i được trải phổ bằng một mã trải phổ giả nhiễu. Kết quả của việc trải phổ là phổ của tín hiệu được trải rộng ra gấp hàng trăm lần so với ban đầu và mật độ năng lượng phổ cũng thấp xuống làm cho giống nhiễu. Chính vì vậy, đối với các máy thu trái phép của những kẻ nghe lén thông tin thì khi thu được những tín hiệu như vậy sẽ chỉ nhận biết được đây là nhiễu hoặc tạp âm. Trên hình 3.15 thể hiện ví dụ về một hệ thống thông tin trải phổ. Theo đó, phổ của tín hiệu sau khi được xử lý qua các bước như nén dữ liệu, mã hóa sửa sai, sau đó sẽ được trải rộng đến băng tần cần thiết bằng cách nhân tín hiệu với chuỗi giả ngẫu nhiên (chuỗi PN) tạo ra từ khối tạo chuỗi PN. Tiếp theo, tín hiệu qua bộ điều chế chuyển phổ này tới băng tần truyền dẫn. Tín hiệu đã điều chế được khuếch đại công suất (KĐCS) và phát trên kênh truyền dẫn mặt đất hoặc kênh vệ tinh.

- Khi đến máy thu *B*, máy thu sẽ được giải điều chế, giải trải phổ, giải mã, giải nén để thu được tín hiệu ban đầu. Để tách được tín hiệu cần thiết thì cần có sự đồng bộ chuỗi PN giữa đầu thu và đầu phát. Việc đồng bộ này được thực hiện nhờ khối đồng bộ chuỗi.

Việc đồng bộ được thiết lập ban đầu và thực hiện liên tục trong suốt quá trình truyền dữ liệu.



Hình 3.15. Sơ đồ chức năng của hệ thống thông tin trải phổ

b) Nhóm các phương pháp trải phổ

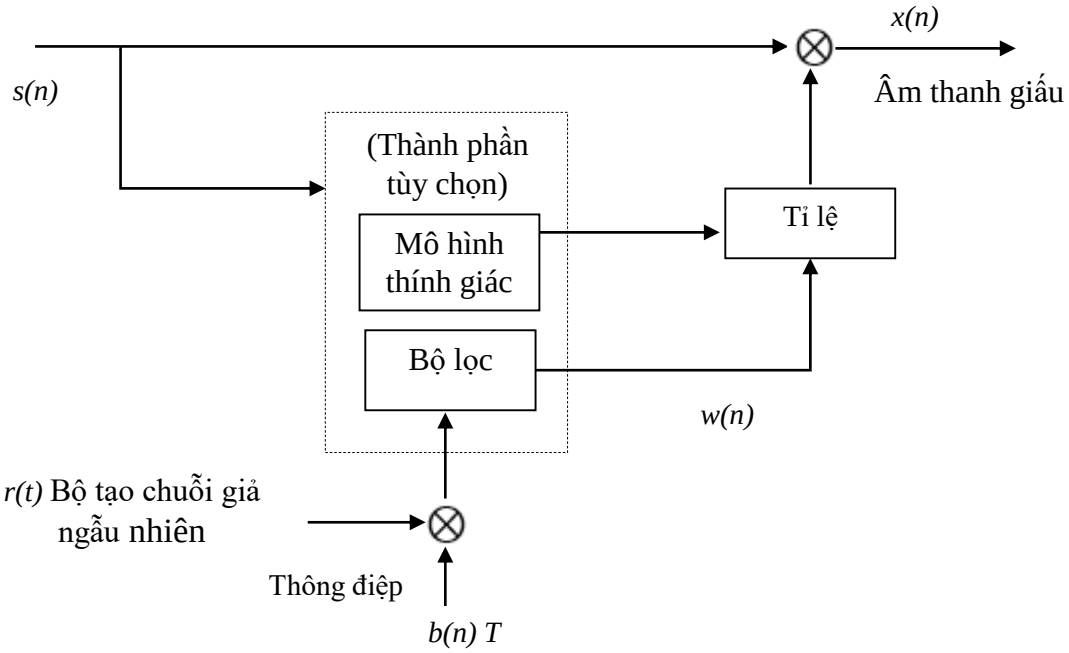
- Phương pháp trải phổ truyền thống là phương pháp dựa trên việc đồng bộ giữa tín hiệu âm thanh giấu và chuỗi giả ngẫu nhiên. Ý tưởng của phương pháp trải phổ truyền thống được thể hiện như hình 3.16. Từ hình 3.16 thấy được nguyên tắc hoạt động của phương pháp trải phổ truyền thống như sau [21, 22]: Thông điệp nhị phân *v={0,1}* hoặc biến có hai giá trị đối cực nhau *b= {1, -1}* được điều chế bằng chuỗi giả ngẫu nhiên *r(n)* dựa vào khóa bí mật. Thông điệp sau khi được điều chế *w(n)* được lấy tỉ lệ dựa vào mức năng lượng cho phép của tín hiệu âm thanh gốc *s*(*n*). Hệ số tỉ lệ α dùng để điều chỉnh mối tương quan giữa hai tính chất bền vững và không nghe thấy. Tin giấu sau khi điều chế *w(n)* có giá trị bằng *r(n)* hay không là phụ thuộc vào *v là 1* hay *v là 0*. Tiếp theo tín hiệu đã điều chế được đưa vào tín hiệu âm thanh gốc để tạo tín hiệu *x(n)*. Tín hiệu *x(n)* được tính theo công thức 3.6 như sau:

$$x(n) = s(n) + \alpha w(n) \tag{3.6}$$

Để trích xuất được thông tin bằng kỹ thuật trải phổ truyền thống thì cần phải đồng bộ giữa *x(n)* và *r(n)*. Công thức đồng bộ giữa *x(n)* và *r(n)* được mô tả như công thức 3.7*:*

$$c = \frac{1}{N}\sum_{i=1}^{N} x(i) \times r(i) \quad (3.7)$$

Trong đó, *N* là kích thước file âm thanh.



Hình 3.16. Ý tưởng trải phổ truyền thống

- Phương pháp trải phổ cải tiến: Về cơ bản, phương pháp trải phổ cải tiến có nguyên tắc hoạt động giống với trải phổ truyền thống. Chỉ khác ở chỗ, các phương pháp trải phổ cải tiến sẽ tìm cách nâng cao hiệu quả của trải phổ truyền thống theo một số hướng chính là [19, 23]: cực đại hóa tính bền vững, cực đại hệ số tương quan và hằng số bền vững. Đặc biệt, trong nghiên cứu [23], đề xuất kỹ thuật chuyển tín hiệu gốc thành nguồn giao thoa làm tăng tính bền vững của quá trình trích rút thông tin. So với phương pháp truyền thống thì trải phổ cải tiến đã có sự khác biệt như công thức 3.8:

$$s = x + \mu(cx, b)u \quad (3.8)$$

Trong đó $\mu(cx, b)u$ là hàm nhúng của $cx = \frac{\langle x,u \rangle}{[\![u]\!]}$. Dễ nhận thấy trải phổ truyền thống là một trường hợp đặc biệt của phương pháp trải phổ cải tiến khi mà μ độc lập với *x* thì sẽ có $\mu(x, b) = b$. Một hướng tiếp cận của trải phổ cải tiến là "Xấp xỉ tuyến tính cho μ". Đây là một phiên bản đơn giản của trải phổ cải tiến bằng cách giới hạn μ là 1 hàm tuyến tính. Công thức trải phổ cải tiến trở thành (xem công thức 3.9):

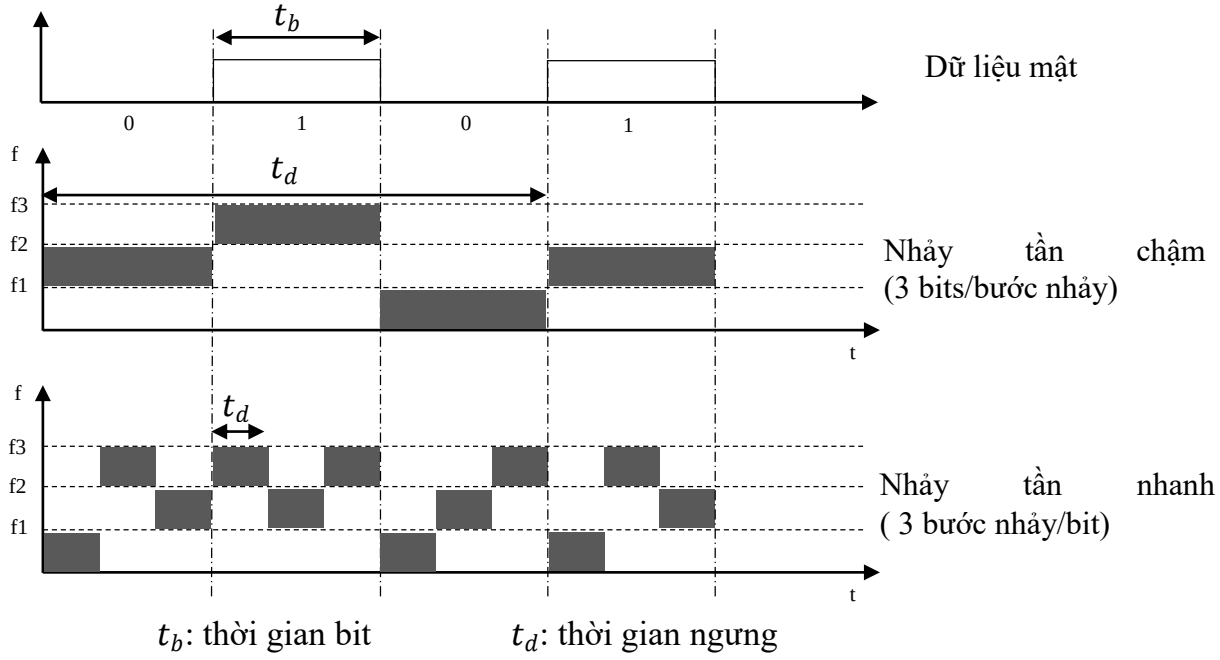
$$x = s + (\alpha b - \lambda x)u \quad (3.9)$$

Các tham số α và λ kiểm soát mức độ biến dạng và loại bỏ biến dạng sóng, trải phổ truyền thống thu được khi cho α = 1 và λ = 0.

c) Các kỹ thuật trải phổ sử dụng để giấu tin trong âm thanh

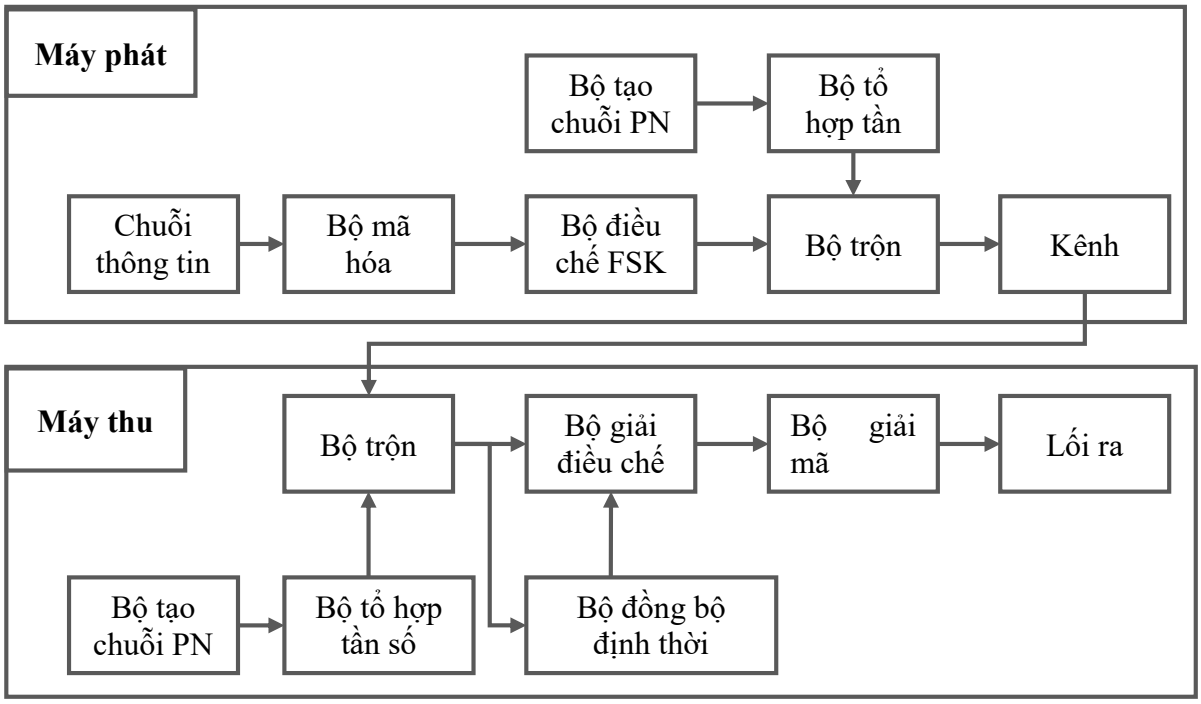
Có 4 kiểu trải phổ phổ biến đang được ứng dụng là: trải phổ trực tiếp DSSS (Direct Sequency Spread Spectrum), nhảy tần (Frequency Hopping Spread Spectrum- FHSS), nhảy thời gian và hệ lai. Nhưng hai phương pháp trải phổ sử dụng trong việc giấu tin trong âm thanh là DSSS và FHSS. Tiếp theo, giáo trình sẽ trình bày chi tiết về cách thức tiến hành giấu tin trong âm thanh sử dụng các phương pháp DSSS và FHSS.

- Phương pháp FHSS: Trải phổ nhảy tần là một công nghệ sử dụng bộ phát tần số và có thể thay đổi tần số truyền một cách đột ngột trong dãy băng tần sử dụng [18]. Trong trải phổ nhảy tần, độ rộng băng thông sẵn có sẽ được chia thành một số lớn các khe tần không lấn lên nhau. Tại bất kì khoảng thời gian nào, tín hiệu truyền đi đều chiếm một hay nhiều hơn một khe tần số nói trên. Việc chọn một khe hay nhiều khe tần số trong một khoảng thời gian truyền tín hiệu đều được thực hiện một cách giả ngẫu nhiên theo tín hiệu ra của một bộ tạo chuỗi giả ngẫu nhiên. Dựa trên tốc độ nhảy của tần số thì phương pháp trải phổ nhảy tần được chia làm 2 loại đó là trải phổ nhảy tần nhanh và trải phổ nhảy tầm chậm. Trong đó, trải phổ nhảy tần nhanh có đặc điểm là tốc độ nhảy nhanh hơn tốc độ dữ liệu. Còn trải phổ nhảy tần chậm thì có tốc độ nhảy chậm hơn tốc độ dữ liệu. Hình 3.17 mô tả ví dụ của trải phổ nhảy tần nhanh và trải phổ nhảy tần chậm.



Hình 3.17. Minh hoạ về trải phổ nhảy tần nhanh và trải phổ nhảy tần chậm

Nhìn chung thì cả hai phương pháp này chỉ khác nhau về tốc độ nhảy, còn nguyên lý hoạt động của hai phương pháp tương tự nhau. Hình 3.18 mô tả về nguyên lý giấu tin và tách tin trong âm thanh sử dụng hệ thống trải phổ nhảy tần.



Hình 3.18. Quy trình giấu tin và tách tin trong âm thanh sử dụng hệ thống trải phổ FHSS

Từ sơ đồ hoạt động của trải phổ nhảy tần trên hình 3.18 có thể thấy quy trình giấu tin của hệ thống trải phổ FHSS cũng sẽ nhận dữ liệu vào gồm 2 thanh phần chính là thông tin cần giấu và bộ chuỗi giả ngẫu nhiên. Trong đó, thông tin cần giấu được đưa vào Bộ mã hóa. Tại đây, tín hiệu được mã hóa bằng khóa riêng trước khi được đưa vào Bộ điều chế. Đây là bước tùy chọn, nghĩa là tùy người gửi tin cài đặt cho máy phát lựa chọn có mã hóa hay không, nếu có thì chọn kỹ thuật mã hóa nào. Tín hiệu sau khi được mã hóa sẽ được đưa vào bộ điều chế FSK (điều chế số theo tần số tín hiệu) để điều chế thành tín hiệu nhị phân *x(t)*. Trong mỗi bit *x(t)* có một trong hai tần số là: $f' = (f' + (2k)\Delta f)$ và $(f' + \Delta f) = (f' + (2k+1)\Delta f)$ tương ứng với bit dữ liệu 0 và bit dữ liệu 1, với $k \in N$. Bộ điều chế FSK sẽ chọn một trong hai tần số: f' và $(f' + \Delta f)$ tương ứng với việc truyền đi bit dữ liệu 0 hay bit dữ liệu 1. Ví dụ sau đây biểu diễn trải phổ nhảy tần chậm. Dữ liệu mã hoá sử dụng MFSK với m=4:

$$s(t) = A\cos(2\Pi f_i t);\ 1 \le i \le m \qquad (3.10)$$

Các tham số trong công thức 3.10 như sau:

$f_i = f_c + (2i - 1 - m)f_d$

f_c: *tần số sóng mang*

f_d: *khoảng cách giữa 2 tần số gần nhất*

m: số phần tử tín hiệu khác nhau = 2^L

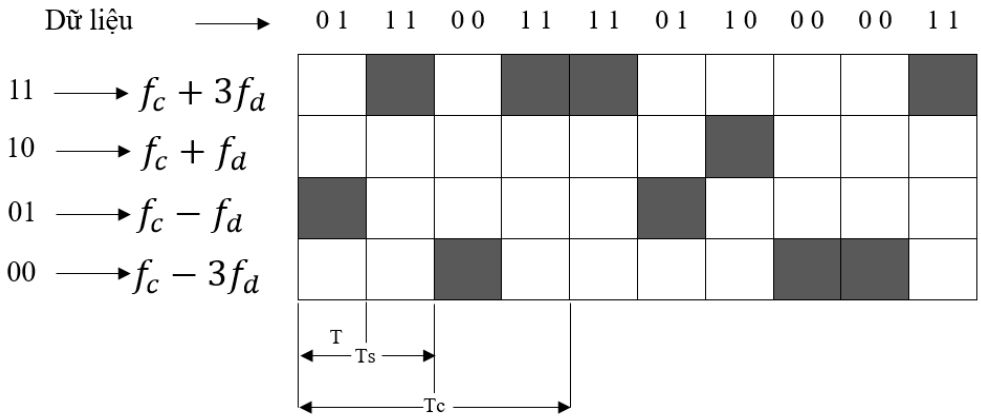
L: Số bit trên mỗi phần tử tín hiệu.

Đối với tốc độ dữ liệu là R, thời lượng của một bit là $T = 1/R$. Tín hiệu MFSK được dịch sang tần số mới mỗi T_s giây: $T_s = L$ x T (T: thời gian của 1 bit). Ví dụ đang xét đối với

trải phổ nhảy tần chậm nên lấy $T_c=2T_s$. Từ đó có các bảng biểu diễn như bảng 3.2. Từ bảng 3.2 này hình 3.19 sẽ thể hiện ví dụ về quá trình giấu tin sử dụng trải phổ nhảy tần chậm.

Bảng 3.2. Ví dụ trải phổ nhảy tần chậm

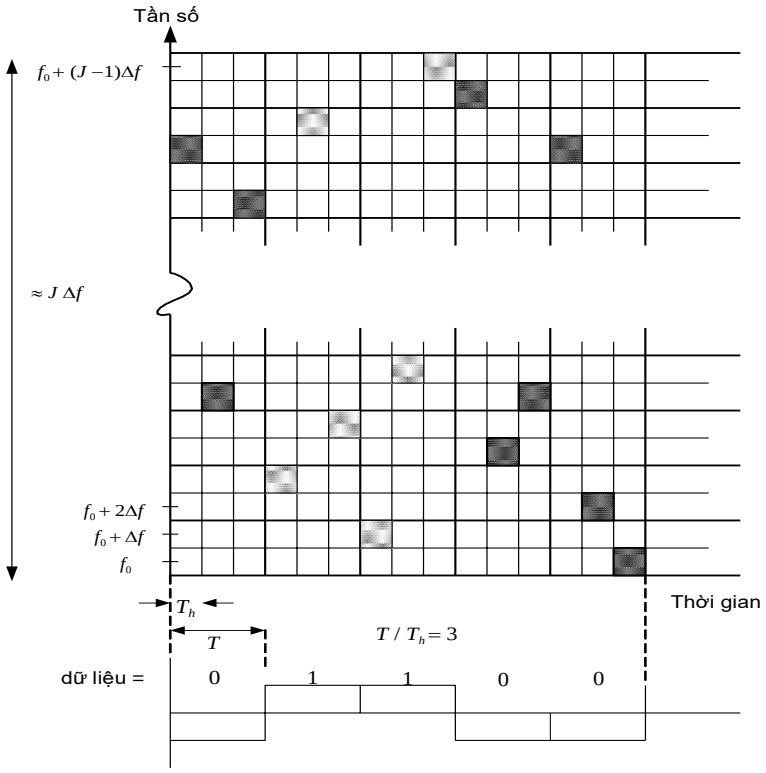
i	f_i	Dữ liệu
1	$F1 = f_c - 3f_d$	00
2	$F2 = f_c - f_d$	01
3	$F3 = f_c + f_d$	10
4	$F4 = f_c + 3f_d$	11



Hình 3.19. Ví dụ về giấu tin dựa trên trải phổ nhảy tần chậm

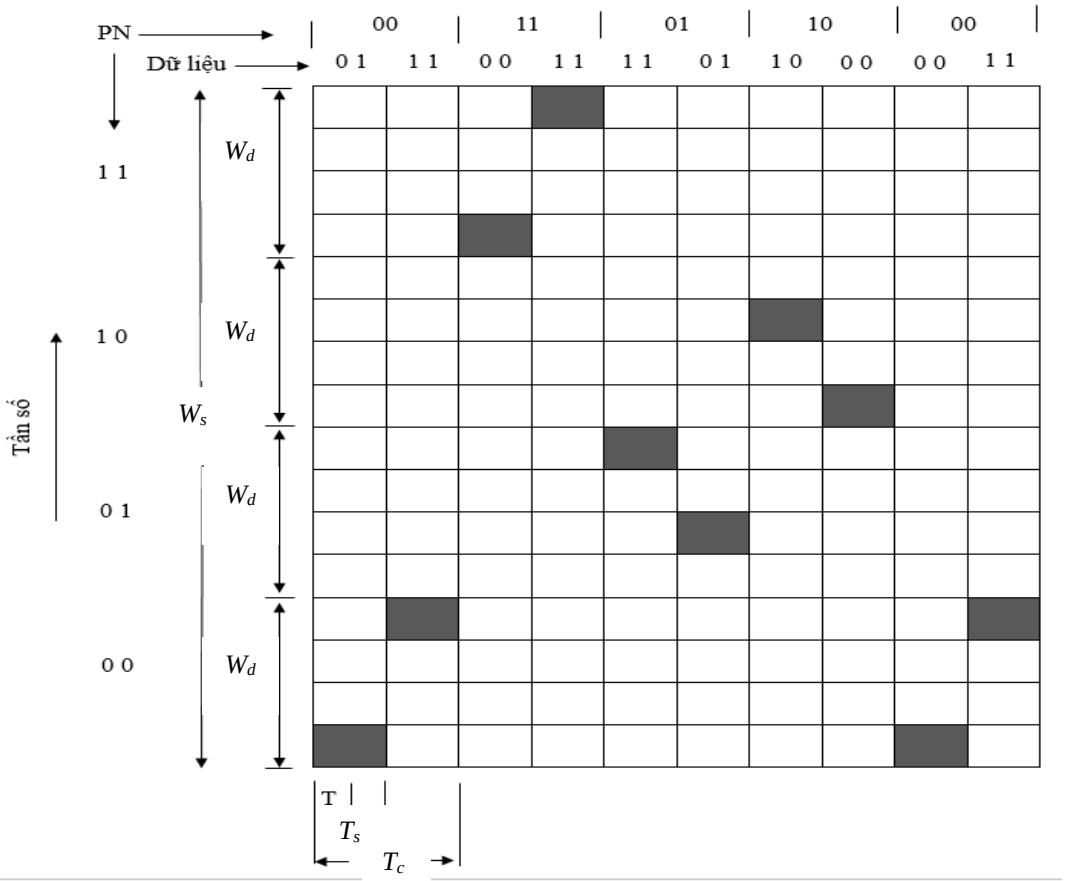
Tương tự như vậy, hình 3.20 thể hiện ví dụ về quá trình giấu tin sử dụng kỹ thuật trải phổ nhảy tần nhanh.

Trên hình 3.20 có T là độ dài bit dữ liệu, T_h là độ dài 1 lần nhảy. Ở ví dụ này, $T = 3T_h$. Δf là giãn cách tần số giữa 2 tần số lân cận. Đối với hệ thống nhảy tần nhanh, do sự thay đổi nhanh tần số sóng mang, giải điều chế liên kết (coherent) là không thực tế nên giải điều chế không liên kết được sử dụng thay. Do đó Δf thường được chọn $=1/T_h$, nghĩa là sử dụng tập tín hiệu trực giao để chất lượng tín hiệu tốt hơn (xác suất lỗi bit ít hơn so với tập không trực giao). Theo đó, giả sử mỗi lần nhảy T_h giây, một trong J tần số được phát đi, tần số phát trong mỗi lần nhảy được chỉ bởi ô có tô nhạt khi bít dữ liệu là 1 hoặc bởi ô có tô đậm khi bít dữ liệu là 0. Khi di chuyển theo chiều ngang trên biểu đồ, có thể thấy rằng tần số phát thay đổi cứ mỗi T_h giây. Sau quá trình xử lý này, thông tin cần giấu sẽ tiếp tục qua bộ trộn tín hiệu.



Hình 3.20. Biểu đồ tần số của tần nhanh với FSK

Từ hình 3.18 thấy được rằng bộ trộn tín hiệu sẽ không chỉ nhận thông tin cần giấu mà còn có chuỗi giả ngẫu nhiên. Trong phương pháp giấu tin này, chuỗi giả ngẫu nhiên là một danh sách của nhiều tần số mà sóng mang có thể nhảy để chọn tần số truyền. Khi danh sách tần số đã nhảy hết, bên truyền sẽ lặp lại từ đầu danh sách này. Tại các thời điểm có sự nhảy tần thì bộ tạo chuỗi giả ngẫu nhiên này sẽ tạo ra một đoạn chứa *m* bit của mã để điều khiển bộ tổng hợp tần số nhằm tạo ra các giá trị tần số nhảy tần cho sóng mang. Sau khi tạo ra đoạn mã có độ dài *m* bit, đoạn mã này được gửi đến bộ tổ hợp tần số. Tại bộ tổ hợp tần số: Sau khi nhận được tín hiệu điều khiển từ bộ tạo chuỗi, bộ tổ hợp tần số tạo ra các giá trị tần số nhảy tần cho sóng mang và nhảy sang hoạt động ở một tần số tương ứng với đoạn mã *m* bit của mã đưa vào, gọi là *y(t)*. Ứng với *m* bit thì mã sẽ cho ra 2^m giá trị tần số khác nhau, đoạn *m* bit này được gọi là một từ tần số và có 2^m giá trị tần số khác nhau. Tần số *y(t)* thay đổi cứ mỗi *T* giây theo các giá trị *m* bit từ bộ tạo chuỗi. Tiếp theo các tín hiệu *x(t)* và *y(t)* sẽ đi vào bộ trộn tín hiệu. Bộ trộn tín hiệu có nhiệm vụ trộn *x(t)* và *y(t)* để tạo ra các tần số tổng và hiệu, một trong hai tần số này sẽ được lọc ra bởi bộ lọc BPF (là bộ lọc chỉ cho các thành phần có tần số trong một dải đi qua, các thành phần lớn hơn hoặc bé hơn đều bị giữ lại) trước khi được đưa lên kênh truyền. Tại kênh truyền: tín hiệu khi được đưa lên kênh có thể gây ra giảm chất lượng như: nhiễu, tạp âm, suy hao công suất tín hiệu... Xét ví dụ về trải phổ nhảy tần chậm như trong bảng 3.2 các tín hiệu được truyền trên kênh truyền như hình 3.21.



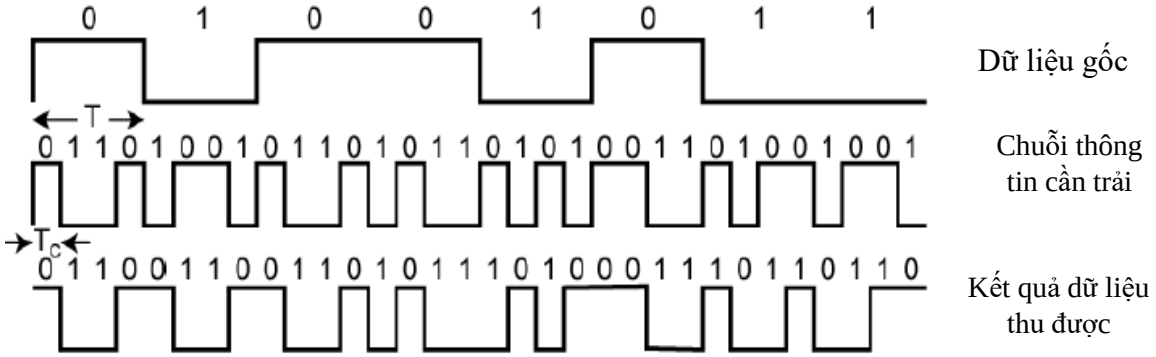
Hình 3.21. Ví dụ về trải phổ nhảy tần chậm

Quy trình tách tin: tín hiệu từ kênh truyền sau khi thu về sẽ được đưa vào bộ trộn. Nhận được tín hiệu truyền về, bộ tạo chuỗi ngẫu nhiên sẽ tạo nên chuỗi giả ngẫu nhiên đồng bộ với chuỗi tới. Chuỗi giả ngẫu nhiên sau khi được tạo ra sẽ được gửi đến bộ tổ hợp tần số để tạo ra các giá trị nhảy tần cho sóng mang, điều khiển lối ra của bộ này. Tín hiệu tần số được tạo ra từ bộ tổ hợp tần số được gửi đến bộ trộn. Tại đây, tín hiệu thu về từ kênh truyền sẽ được trộn với tín hiệu lối ra của bộ tổ hợp tần số, dựa theo dải tần lọc của bộ lọc BPF mà thu được tín hiệu *x(t)*. Tín hiệu này được gửi đồng thời cho bộ giải điều chế FSK và bộ đồng bộ định thời để đồng bộ về mặt thời gian. Tại FSK, tín hiệu sóng mang *x(t)* được giải điều chế để tái tạo lại dữ liệu. Cuối cùng dữ liệu này sẽ giải mã để khôi phục lại dữ liệu gốc ban đầu thông qua bộ giải mã.

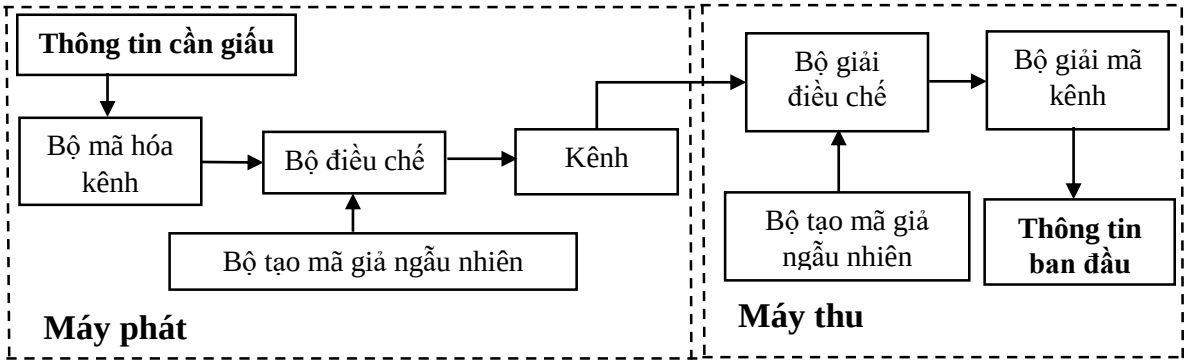
Từ quy trình giấu tin và tách tin trong âm thanh sử dụng kỹ thuật trải phổ nhảy tần có thể thấy rằng, phương pháp này có ưu điểm là có khả năng chống nhiễu băng hẹp cao vì tín hiệu nhảy sang một dải tần số khác do đó làm cho nó khó bị đánh cắp hoặc tấn công. Ngoài ra, FHSS có tính linh hoạt cao có thể sử dụng băng thông một cách hiệu quả hơn so với các phương pháp truyền thông không dây khác. Bởi vì nó chỉ sử dụng một phần nhỏ của băng thông tần số có sẵn hoặc có thể dễ dàng thêm các kênh tần số mới hoặc mở rộng phạm vi truyền dẫn. Mặc dù vậy, phương pháp trải phổ nhảy tần cũng có tồn tại khuyết điểm là khi

kênh truyền tin có giao thức mã hóa được đặt trên một giải tần có nhiều tần số nhiễu, sẽ khó đảm bảo toàn vẹn chất lượng của thông tin được gửi đi từ máy phát, từ đó gây khó khăn cho việc giải mã thông điệp nhận được ở phía máy thu. Ngoài ra, phương pháp này đòi hỏi việc cấu hình và đồng bộ phức tạp để đảm bảo tính ổn định và độ tin cậy.

- Phương pháp DSSS: DSSS là một phương pháp truyền dữ liệu trong đó hệ thống truyền và nhận đều sử dụng một tập các tần số có độ rộng 22 MHz. Trải phổ dãy trực tiếp được thực hiện bằng cách áp dụng một tín hiệu trải phổ phụ là dãy có tần số cao hơn khối dữ liệu cần truyền lên tín hiệu gốc. Việc phân phối tín hiệu phụ này trên băng tần truyền tải sẽ giúp tăng độ rộng của băng tần và giảm độ nhiễu. Hình 3.22 mô tả ví dụ về dãy trải phổ trực tiếp. Hình 3.23 trình bày nguyên tắc giấu tin và tách tin trong âm thanh sử dụng kỹ thuật trải phổ trực tiếp.



Hình 3.22. Minh họa trải phổ dãy trực tiếp

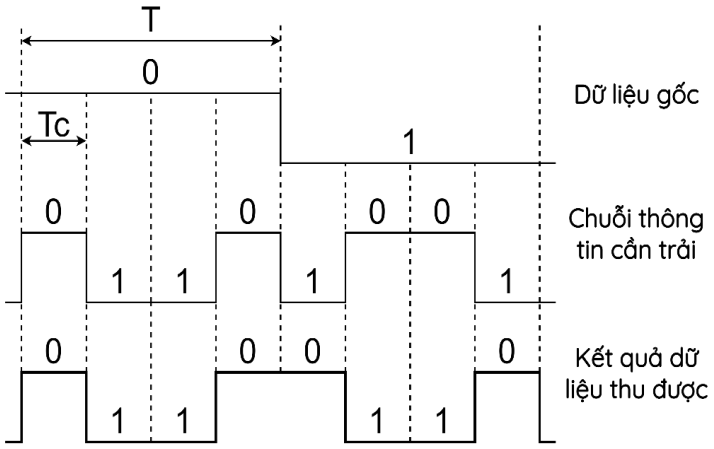


Hình 3.23. Nguyên tắc giấu tin và tách tin trong âm thanh dựa trên DSSS

Nguyên tắc giấu tin sử dụng kỹ thuật trải phổ trực tiếp như sau: Trước tiên dữ liệu cần giấu được mã hóa bằng bộ mã hóa kênh để đưa vào các bit dư nhằm mục đích phát hiện hay sửa các lỗi có thể phát sinh khi truyền dẫn tín hiệu qua kênh tần số vô tuyến. Tín hiệu sau khi được mã hóa bằng bộ mã hóa kênh được đưa vào bộ điều chế. Tại bộ điều chế có hai quá trình diễn ra đó là quá trình trải phổ và quá trình điều chế sóng mang. Trong một

số tài liệu quá trình trải phổ và điều chế có thể bị tách riêng (không cùng nằm trong bộ điều chế) và thứ tự thực hiện trước sau không đồng nhất. Tuy nhiên trên thực tế thì hai quá trình này thường được kết hợp và thực hiện ở một khối duy nhất, thứ tự thực hiện có thể tráo đổi cho nhau, việc này không làm ảnh hưởng đến kết quả của tín hiệu đầu ra. Vì vậy, tại đây cả hai quá trình được đặt trong bộ điều chế. Giả sử quá trình trải phổ được thực hiện trước quá trình điều chế sóng mang, quy trình tiền xử lý tín hiệu sẽ được diễn ra như sau: Sau khi nhận được tín hiệu đã được mã hóa từ bộ mã hóa kênh và chuỗi giả ngẫu nhiên từ bộ tạo mã giả ngẫu nhiên, bộ điều chế sẽ thực hiện trải phổ bằng cách nhân hai tín hiệu này với nhau. Cụ thể, với dữ liệu có *n* bit và chuỗi giả ngẫu nhiên có *nT* bit, 1 bit của dữ liệu ban đầu sẽ kết hợp với *T* bit của chuỗi giải ngẫu nhiên để cho ra chuỗi kết quả. Ví dụ với dữ liệu ban đầu là 01 (*n = 2, T =4*). Hình 3.24 thể hiện ví dụ về quá trình trải phổ với 2 bit 0 và 1.

A	B	XOR
0	0	0
0	1	1
1	0	1
1	1	0



Hình 3.24. Ví dụ minh họa về quá trình trải phổ được thực hiện với 2 bit 0 và 1

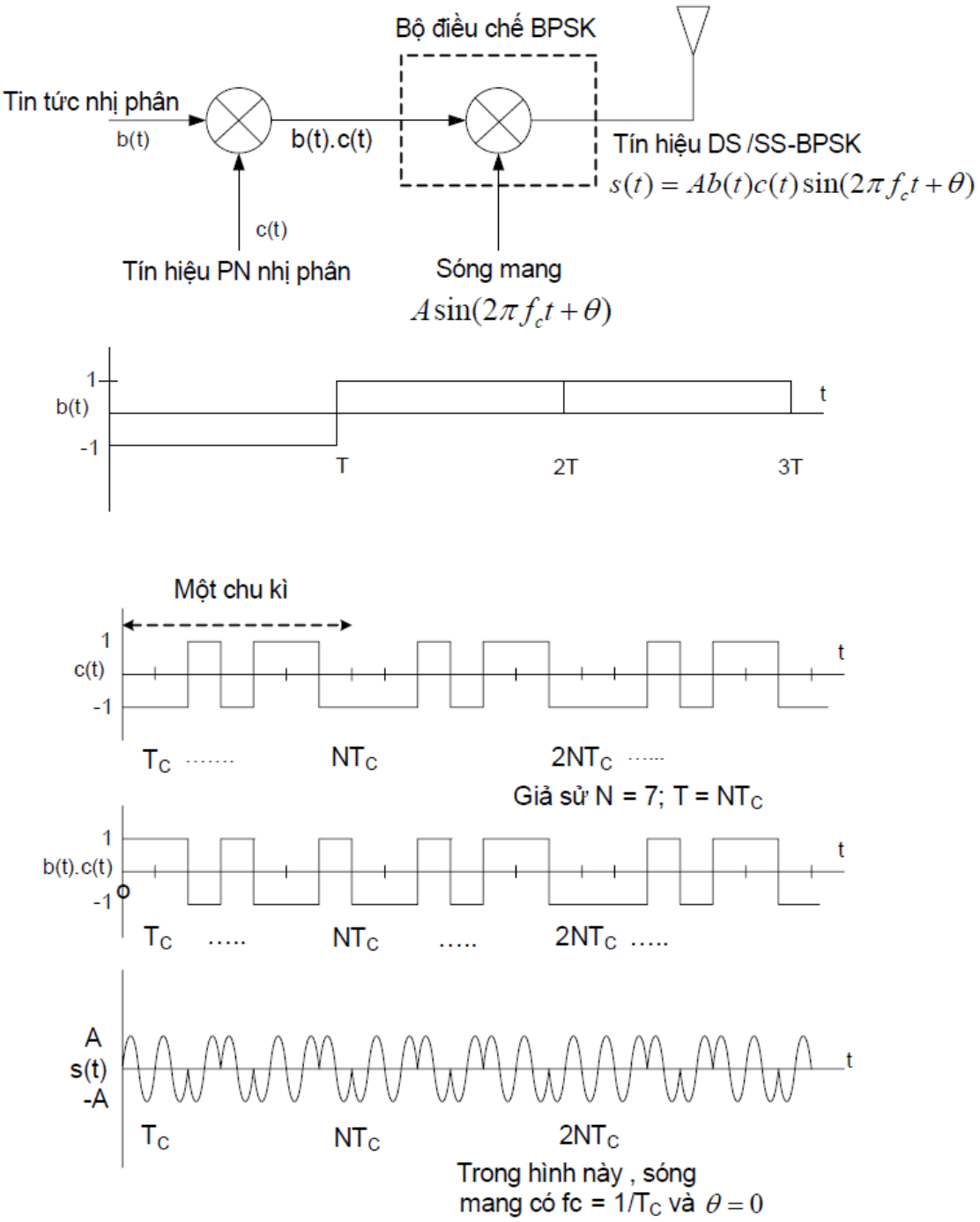
Kết quả là phổ của tín hiệu nhận được sẽ được trải ra trên dải không mong muốn dựa vào chuỗi giả ngẫu nhiên. Sau đó phổ của tín hiệu được dịch đến dải tần phát bằng phương pháp BPSK hoặc QPSK (đây là quá trình điều chế sóng mang theo phương pháp BPSK hoặc QPSK). BPSK là phương pháp chia đường tròn lượng giác thành 2 cung, độ dài của hai cung được tùy chỉnh theo. Mỗi cung sẽ biểu diễn cho một trạng thái của bit 0 và bit 1. Về mặt toán học, BPSP sẽ có công thức toán học như sau (xem công thức 3.11):

$$A\sin(2\pi f_c t + \theta) \tag{3.11}$$

QPSK là một phương pháp chia đường tròn thành 4 cung có độ dài có thể được tùy chỉnh. 4 cung thành sẽ biểu diễn cho trạng thái của 2 bit 1 (00, 01, 11, 10). Hình 3.25 mô tả ví dụ minh họa cho bộ điều chế BPSK. Trong ví dụ này, quá trình trải phổ được diễn ra trước quá trình điều chế sóng mang. Tín hiệu sau khi điều chế sẽ được phát qua kênh truyền dẫn, kênh này có thể là kênh dưới đất hoặc kênh vệ tinh. Các kênh truyền dẫn đó có thể gây ra giảm chất lượng như: nhiễu, tạp âm, suy hao công suất tín hiệu.

Đối với quá trình tách tin: tín hiệu sau khi được lấy trên kênh truyền dẫn sẽ được đưa vào bộ giải điều chế. Tại bộ giải điều chế, bộ tạo mã giả ngẫu nhiên sẽ tạo nên chuỗi giả

ngẫu nhiên đồng bộ với chuỗi tới nhằm giải trải phổ cho tín hiệu thu được từ kênh truyền. Tín hiệu sau khi được giải trải phổ sẽ được giải điều chế sóng mang bằng phương pháp BPSK hoặc QPSK để thu được tín hiệu băng gốc. Tín hiệu băng gốc này sẽ được truyền đến bộ giải mã kênh để giải mã, lấy ra tín hiệu gốc. Lưu ý rằng, quá trình tách tin này có thể sử dụng thêm bộ nén/giải nén dữ liệu hoặc bộ mã sửa sai/ giải mã. Chúng dùng để cải thiện chất lượng hệ thống.



Hình 3.25. Bộ điều chế BPSK

d) Nhận xét về phương pháp

Nhìn chung, phương pháp giấu tin trong âm thanh dựa trên kỹ thuật trải phổ trực tiếp có ưu điểm là độ bảo mật và khả năng chống nhiễu cao do khi trải phổ năng lượng của tín hiệu được phân bố rộng rãi trên dải tần do đó đã giảm độ nhạy cảm với nhiễu sóng. Ngoài ra, phương pháp này có thể giấu được lượng thông tin lớn mà vẫn giữ nguyên được chất lượng âm thanh. Đặc biệt, về mặt ứng dụng phương pháp này thường được áp dụng trong các ứng dụng yêu cầu tính bí mật cao và cho phép nhiều thiết bị sử dụng cùng một dải tần số mà không cần phân bổ tần số riêng biệt cho mỗi thiết bị do đó tận dụng hiệu quả tài nguyên. Mặc dù vậy, phương pháp này có nhược điểm là độ trễ lớn và yêu cầu cao về phần cứng. Cụ thể, để thực hiện giấu tin và tách tin, phần cứng của thiết bị truyền thông phải có khả năng xử lý tín hiệu nhanh và chính xác, dẫn đến chi phí đầu tư cao. Ngoài ra, cũng có một số nghiên cứu chỉ ra rằng, phương pháp trải phổ nhảy tần có thể bị phá vỡ bởi các kỹ thuật phân tích tín hiệu như phân tích dữ liệu phổ và phân tích dữ liệu thời gian [19]. Các kỹ thuật trải phổ hiện nay đang được ứng dụng rất rộng rãi và đặc biệt là kỹ thuật này đang được sử dụng trong nhiều ứng dụng mới, như mạng thông tin cá nhân (Personal Communication Networks), WLAN, tổng đài nhánh cá nhân vô tuyến (Wireless Private Branch Exchanges), các hệ thống điều khiển kiểm kê vô tuyến, các hệ thống báo động trong tòa nhà và hệ thống định vị toàn cầu (Global Positioning System) [19].

3.4.3. Phương pháp Echo

a) Định nghĩa

Tiếng vang là sự phản xạ của âm thanh đến người nghe có độ trễ so với âm thanh trực tiếp. Sự chậm trễ này tỷ lệ thuận với khoảng cách của bề mặt phản chiếu từ nguồn và người nghe. Ví dụ điển hình là tiếng vang được đáy giếng, tòa nhà, hoặc các bức tường của một căn phòng kín tạo ra. Một tiếng vang thực sự là một âm phản chiếu duy nhất của nguồn âm thanh. Tai của con người không thể phân biệt được đâu là tiếng vang và đâu là âm thanh trực tiếp ban đầu nếu độ trễ này nhỏ hơn 1/15 giây. Sức mạnh của tiếng vang thường được đo bằng dB áp suất âm thanh so với sóng truyền trực tiếp.

Kỹ thuật giấu tin bằng phương pháp Echo (tiếng vang) được thực hiện bằng cách thêm tiếng vang vào trong tín hiệu gốc. Phương pháp này dựa vào đặc trưng của hệ thống thính giác con người khi không phân biệt được hai âm thanh nếu chúng xảy ra gần như đồng thời, có độ lệch trong khoảng từ 1 đến 40 mili giây. Cụ thể, khi thời gian giữa tín hiệu gốc và tiếng vang giảm xuống, lúc đó hai tín hiệu có thể trộn lẫn làm người nghe không thể phân biệt hai tín hiệu. Hình 3.26 thể hiện một số thành phần trong phương pháp mã hóa tiếng vang.

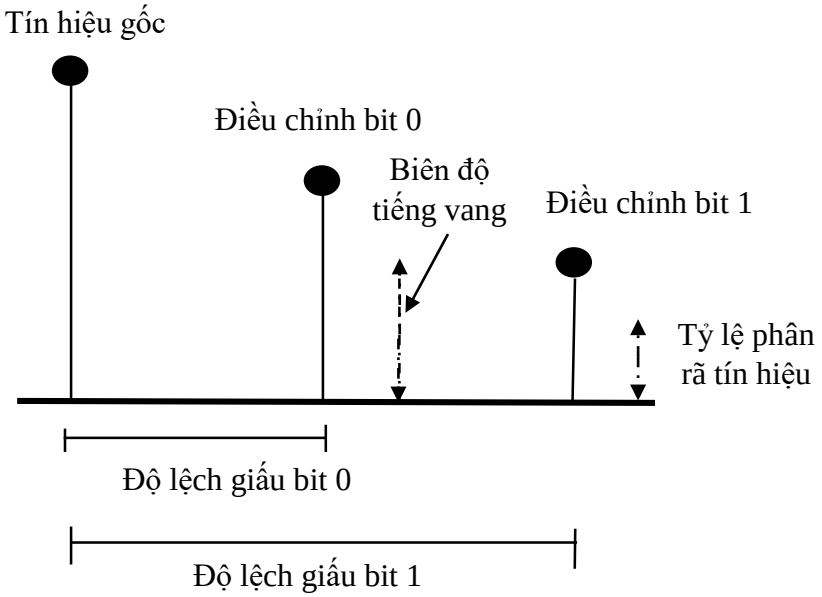
Dựa trên hình 3.26 có thể thấy có ba tham số chính trong quy trình mã hóa tiếng vang bao gồm: Tín hiệu gốc; Tỷ lệ phân rã (Tốc độ phân rã); Độ trễ giữa âm thanh ban đầu và tiếng vang. Cụ thể với phương pháp này thông tin được giấu trong một tín hiệu rời rạc *f(t)* bằng cách thêm tiếng vang $f(t-\Delta t)$ vào tín hiệu chứa *c*(*t*). Công thức tổng quát trong trường hợp này như sau (xem công thức 3.12):

$$c(t) = f(t) + \alpha f(t - \Delta t) \quad (3.12)$$

Trong đó:

Δt là khoảng thời gian dừng giữa tín hiệu phát và tiếng vang. Tại bước mã hóa, người giấu tin có thể chọn các giá trị Δt và $\Delta t'$ tương ứng với các bit 0 hoặc 1 được nhúng. Trong một số bài toán có thể chỉ cần thêm một tiếng vang vào tín hiệu gốc để giấu tin. Tuy nhiên, trong các phương pháp điều chỉnh tiếng vang cải tiến thì có thể thêm nhiều tiếng vang. Tín hiệu vang có thể là vang trước và vang sau so với tín hiệu gốc để giấu tin. Ví dụ trong [14] đề xuất phương pháp thêm tiếng vang cả trước và sau so với tín hiệu gốc như công thức 3.13:

$$c(t) = f(t) + \alpha f(t - \Delta t) + af(t + \Delta t) \quad (3.13)$$



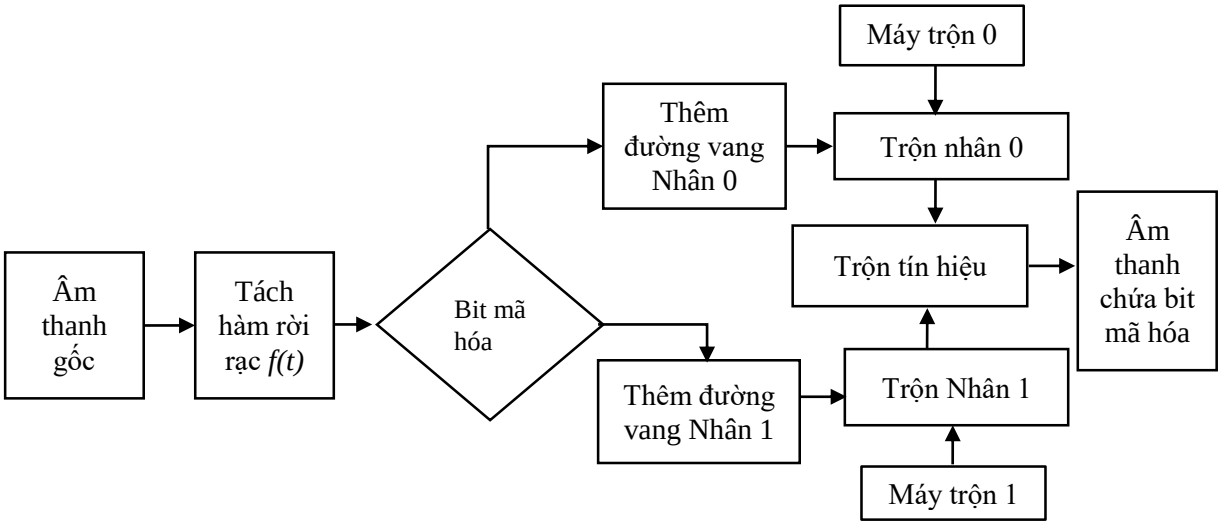
Hình 3.26. Các tham số chính trong phương pháp mã hóa Echo

b) Quy trình giấu tin

Từ sơ đồ tổng quát trên hình 3.27 cho thấy các tham số chính trong quy trình giấu tin sử dụng phương pháp mã hóa tiếng vang gồm:

- Âm thanh gốc: Là tập tin âm thanh gốc sử dụng để thêm tiếng vang.
- Hàm $f(t)$: là hàm rời rạc được tách từ âm thanh gốc.
- Bit mã hóa: Bit được mã hóa để đưa vào trong âm thanh, chỉ là các bit đơn 0 hoặc 1.
- Nhân 0 và Nhân 1: Là các nhân để mã hóa tương ứng với các bit 0 hoặc bit 1. Mỗi nhân 0 hoặc nhân 1 sẽ có các độ trễ khác nhau tùy vào người giấu tin đặt ra.
- Máy trộn: Là các thiết bị, hay phần mềm có khả năng thêm các tín hiệu sin vào một hàm âm thanh.

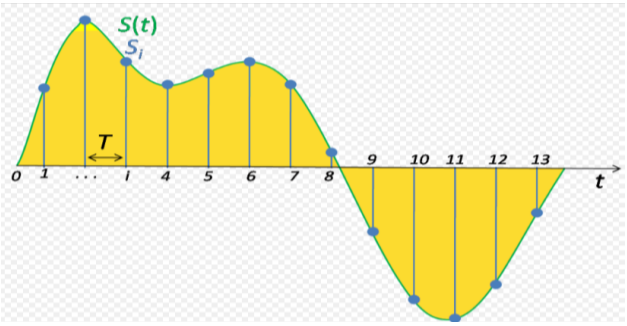
- Trộn tín hiệu: Kết quả nhận được khi đưa tín hiệu vào máy trộn
- Âm thanh chứa bit mã hóa: Là âm thanh sau khi được mã hóa đã có các bit được giấu vào.



Hình 3.27. Sơ đồ tổng quát phương pháp giấu tin trong âm thanh dựa trên mã hóa Echo

Dựa trên các thành phần chính trong sơ đồ tổng quát của phương pháp mã hóa tiếng vang có thể xây dựng quy trình giấu tin sử dụng phương pháp này như sau:

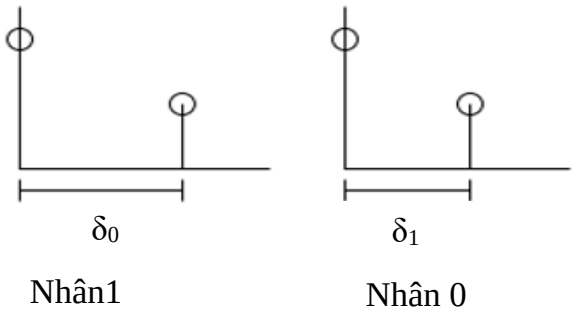
Bước 1: Xử lý tín hiệu âm thanh. Theo đó, âm thanh gốc sẽ được phân tích thành các hàm rời rạc theo thời gian *F(t)*. Một trong những phương pháp để tách hàm rời rạc là phương pháp lấy mẫu bằng cách nhìn tập hợp các điểm trên trục tọa độ không gian và thời gian. Đối với các tín hiệu khác nhau theo thời gian việc lấy mẫu được thực hiện bằng cách đo các giá trị của tín hiệu liên tục ở thời điểm mỗi giây T, T được gọi là khoảng thời gian lấy mẫu. Như vậy, tín hiệu sau khi được lấy mẫu $x[n]$ được đưa ra bởi: $s[n] = s(nT) \quad với\ n = 0, 1, 2, 3, ...$ Hình 3.28 mô tả ví dụ về phương pháp lấy mẫu.



Hình 3.28. Ví dụ về lấy mẫu tín hiệu theo theo hàm liên tục $\boldsymbol{S(t)}$

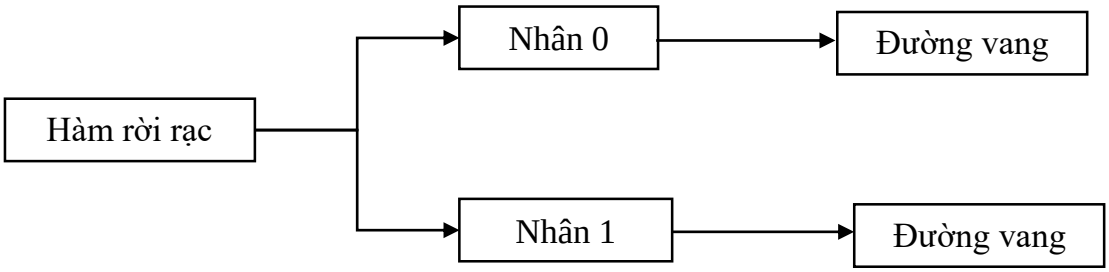
Trên hình 3.28, các tín hiệu liên tục có màu xanh lục còn các mẫu rời rạc có màu xanh lam.

Bước 2: Nhân hệ thống mã hóa. Sử dụng nhân 0 và nhân 1 kết hợp với tín hiệu gốc để tạo ra tiếng vang tương tự tín hiệu gốc nhưng trễ hơn. Hình 3.29 thể hiện ví dụ về độ trễ nhân 0 và nhân 1.



Hình 3.29. Nhân 0 và nhân 1

Nhân 0 có độ trễ là δ_0 và nhân 1 có độ trễ là δ_1, dựa vào độ trễ để xác định tiếng vang so với tín hiệu ban đầu. Nhân 0 để mã hóa bit 0, nhân 1 để mã hóa bit 1. Hình 3.30 mô tả kết quả khi mã hóa nhân 0 và nhân 1.

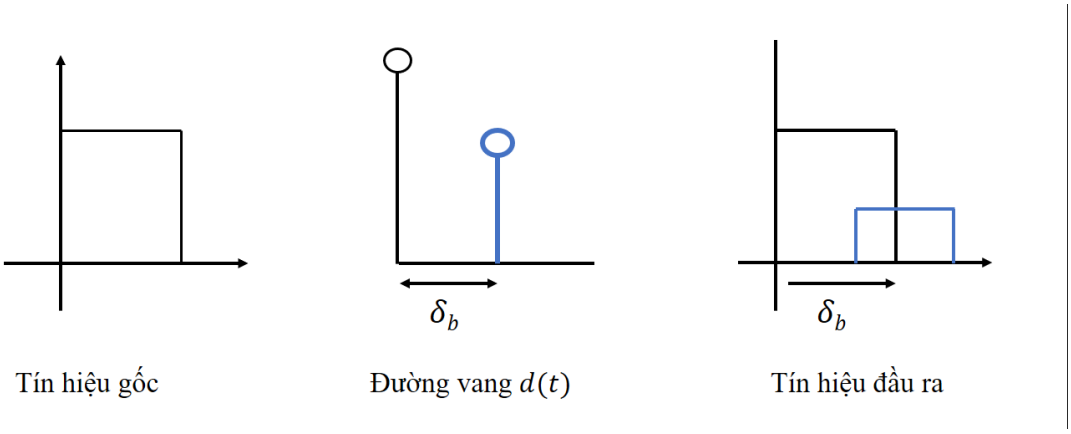


Hình 3.30. Đầu vào và đầu ra bước 2

Từ hình 3.20 thấy được, kết quả thu được là hai đường tiếng vang d_0 và d_1 có dạng:

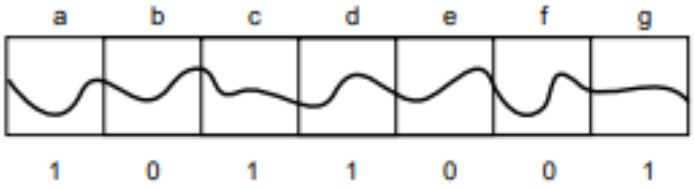
$$d(t) = F(t) + \beta F(t+\Delta t)$$

trong đó: $F(t)$ là hàm rời rạc theo thời gian; β là tỷ lệ phân rã; Δt là độ trễ của tiếng vang so với âm thanh gốc



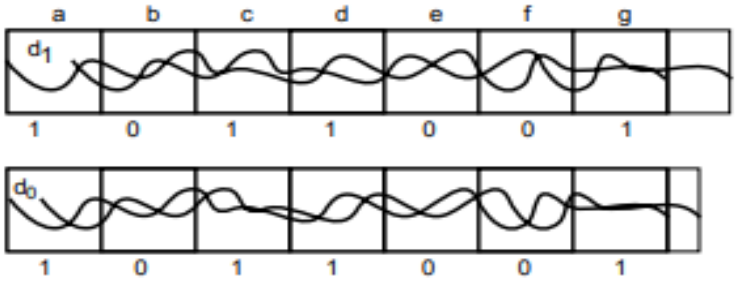
Hình 3.31. Âm thanh khi thêm tiếng vang

Hình 3.31 thể hiện ví dụ về âm thanh trước và sau khi được thêm tiếng vang. Để mã hóa nhiều hơn một bit, âm thanh ban đầu được chia thành từng phần nhỏ hơn. Giả sử phải giấu *N* bit vào âm thanh, *L* là chiều dài của đoạn, *L* được chọn sao cho *N* x *L* không lớn hơn độ dài của tín hiệu âm thanh. Ví dụ: tín hiệu được chia thành 7 phần *a, b, c, d, e, f, g* như trên hình 3.32.



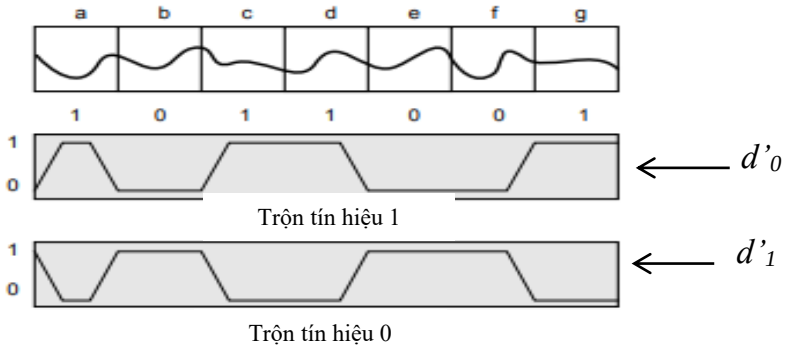
Hình 3.32. Ví dụ giấu bit 0 và bit 1

Từ hình 3.32 thấy được rằng: Các phần *a, c, d, g* chứa các bit 1 phần còn lại chứa bit 0. Theo lý thuyết kỹ thuật mã hóa tiếng vang sẽ mã hóa từng phần và sử dụng từng loại nhân phù hợp với bit cần giấu nhưng trong thực tế các chuyên gia đã mã hóa toàn bộ sử dụng nhân 0 hoặc nhân 1, nên kết quả sẽ thu được hai tiếng vang đó là d_0 và d_1 như hình 3.33.



Hình 3.33. Kết quả tiếng vang sử dụng nhân 0 và nhân 1

Bước 3: Giấu tin. Từ kết quả của bước 2, khi này tiếng vang đã được chia thành các đoạn để chứa các bit cần giấu. Tiếng vang được nhân với hàm trộn theo nguyên tắc: d_0 được nhân với hàm trộn 0, d_1 được nhân với hàm trộn 1. Tức là khi thu được tiếng vang ở bước 2, các tín hiệu này được đưa vào máy trộn riêng để cho ra tín hiệu trộn d'_0 và d'_1. Để thu được tín hiệu trộn d'_0 và d'_1 thì trong máy trộn sẽ tự động sinh ra tín hiệu sin. Kết quả tạo ra 2 tín hiệu trộn có dạng là các đường dốc, tín hiệu trộn 0 là phần bù của tín hiệu trộn 1. Các kết quả này thể hiện qua hình 3.34.



Hình 3.34. Kết quả của hàm trộn

Bước 4: Trộn tín hiệu. Kết hợp 2 tín hiệu trộn thu được tín hiệu mã hóa khi cộng 2 tín hiệu, những đoạn có giá trị bằng 1 là mã hóa bit 1, đoạn có giá trị 0 là mã hóa bit 0, những đoạn có giá trị nằm trong khoảng từ 0 đến 1 là đoạn chuyển tiếp giữa 2 đoạn mã hóa khác nhau (giữa 2 đoạn mã hóa khác nhau 0 và 1). Để hiểu rõ hơn về quá trình giấu tin trong âm thanh dựa trên mã hóa tiếng vang, hãy xét ví dụ dưới đây. Giả sử ban đầu, người giấu tin có đoạn âm thanh gốc với các giá trị lần lượt là: 3, 5, 2, 1, 4. Với các tham số: $\boldsymbol{\delta_1 = 2; \delta_0 = 3; \alpha_0 = \alpha_1 = 0{,}5.}$ Theo đó, Với $\boldsymbol{\delta_1 = 2}$ có kết quả sau khi nhúng bit 1 là: 0, 0, 3, 5, 2. Tiến hành thực hiện giấu âm thanh, thu được kết quả ở từng vị trí như sau:

Giá trị 1: 3 + 0 x 0,5 = 3

Giá trị 2: 5 + 0 x 0,5 = 5

Giá trị 3: 2 + 3 x 0,5 = 3,5

Giá trị 4: 1 + 5 x 0,5 = 3,5

Giá trị 5: 4 + 2 x 0,5 = 5

Kết quả thu được lần lượt là: 3; 5; 3,5; 3.5; 5

Với $\boldsymbol{\delta_0 = 3}$, thu được kết quả sau khi nhúng bit 0 là: 0, 0, 0, 3, 5

Tiến hành thực hiện giấu âm thanh, ta thu được kết quả ở từng vị trí như sau:

Giá trị 1: 3 + 0 x 0,5 = 3

Giá trị 2: 5 + 0 x 0,5 = 5

Giá trị 3: 2 + 0 x 0,5 = 2

Giá trị 4: 1 + 3 x 0,5 = 2,5

Giá trị 5: 4 + 5 x 0,5 = 6,5

Kết quả là: 3; 5; 2; 2,5; 6,5

c) Quy trình tách tin

Thông tin được giấu trong âm thanh bằng cách chèn tiếng vang vào âm thanh gốc với 1 trong 2 khoảng thời gian trễ của tiếng vang. Bit 1 được giấu bằng tiếng vang có độ trễ α_1,

bit 0 được giấu bằng tiếng vang có độ trễ α_0. Việc trích xuất thông tin được giấu liên quan đến việc phát hiện độ trễ của các tiếng vang. Để thực hiện điều này, cần phân tích Cepstrum được sử dụng trong quá trình mã hóa tiếng vang. Quá trình tách tin được thực hiện bằng cách so sánh từng đoạn giữa dữ liệu gốc và dữ liệu mang tin để xác định tách bit 0 hoặc bit 1. Theo đó, âm thanh có chứa tin giấu được chia thành các phân đoạn là số bit ẩn có cùng độ dài phân đoạn như đã được sử dụng trong quá trình mã hóa. Để truy xuất Cepstrum thực (bit ẩn thứ *n* của đoạn thứ *n*) sử dụng công thức 3.13:

$$c_n[i] = ifft(\log(\text{abs}(fft(sn[i])))) \quad (3.13)$$

Sau đó so sánh trên các điểm trễ. Nếu: $c_n[d_0 + 1] > c_n[d_1 + 1]$ thì bit được truy xuất là 0, ngược lại là 1.

Một điểm cần lưu ý trong quá trình tách tin là giai đoạn phân tích Cepstrum. Nếu Cepstrum không có độ chênh lệch lớn tại các thời điểm có tiếng vang được chèn vào nên việc phát hiện ra bit được giấu là rất khó khăn. Để giải quyết vấn đề này, người tách tin cần tính cepstrum tương quan (autocorrelation Cepstrum) thay vì tính Cepstrum thông thường.

d) Nhận xét về phương pháp

Phương pháp giấu tin trong âm thanh bằng kỹ thuật mã hóa tiếng vang có thể giúp bảo mật thông tin truyền tải và tránh bị đánh cắp thông tin bởi kẻ xấu. Ngoài ra, phương pháp này cho phép giấu thông tin vào tín hiệu âm thanh bằng cách tạo ra độ trễ, điều này làm cho thông tin giấu kín rất khó để phát hiện bằng tai người. Mặc dù vậy, phương pháp này có thể bị ảnh hưởng bởi các tác động môi trường như tiếng ồn, dao động nhiễu, các thay đổi về độ dốc và điểm ngưỡng của tín hiệu âm thanh, làm giảm tính ổn định của quá trình giấu tin. Ngoài ra, phương pháp mã hóa tiếng vang yêu cầu quá trình giấu tin và tách tin phức tạp. Cụ thể để truy xuất thông tin giấu, cần phải có một mã hóa đặc biệt để xác định vị trí và độ trễ của các tín hiệu âm thanh được chèn vào, điều này làm cho quá trình giải mã trở nên phức tạp hơn. Để khắc phục một số nhược điểm của phương pháp này, trong một số nghiên cứu khác cũng đã đề xuất một số hướng tiếp cận khác như: chèn tiếng vang lưỡng cực - Bipolar Echo Hiding hoặc phương pháp chèn tiếng vang trước sau – Backward Forward Echo Hiding. Chi tiết các phương pháp này được mô tả chi tiết trong các nghiên cứu [28, 29].

3.5. Tổng kết chương 3

Trong chương 3 giáo trình đã trình bày tổng quan về giấu tin trong âm thanh. Cụ thể, nội dung chương đã bao gồm các vấn đề sau:

- Trình bày một số định nghĩa, khái niệm và các thành phần cơ bản cũng như các yêu cầu tối thiểu đối với kỹ thuật giấu tin trong âm thanh. Các phân tích và đánh giá về các thành phần này sẽ là cơ sở để các kỹ thuật giấu tin trong âm thanh lựa chọn nhằm tiến hành giấu tin sao cho an toàn và phù hợp với yêu cầu sử dụng. Ngoài ra, trong chương này giáo trình cũng đã liệt kê một số định dạng cơ bản của các file âm thanh cũng như một số công cụ hỗ

trợ giấu tin đang có. Dựa trên các công cụ mà giáo trình đã liệt kê, người dùng có thể sử dụng các công cụ đó để thực hành giấu tin và tách tin từ đó giúp hiểu sâu hơn về các kỹ thuật giấu tin trong âm thanh.

- Phân tích và đánh giá quy trình giấu tin và tách tin của một số phương pháp giấu tin trong âm thanh đang được sử dụng phổ biến. Theo đó, ngoài việc đưa ra định nghĩa, khái niệm và đặc điểm của một số phương pháp giấu tin trong âm thanh đang có, giáo trình đã đi vào phân tích ưu điểm và nhược điểm của từng phương pháp. Dựa trên việc phân tích và đánh giá này, giáo trình đã không chỉ cung cấp cho người đọc cái nhìn chi tiết và sâu hơn về một số phương pháp giấu tin đang có mà còn hỗ trợ người dùng trong việc lựa chọn phương pháp và thuật toán giấu tin cho phù hợp với từng mục tiêu và ứng dụng thực tế. Ngoài ra, để hiểu rõ hơn về quy trình cài đặt các thuật toán này bằng công cụ và ngôn ngữ lập trình, độc giả quan tâm có thể tham khảo ở tài liệu [33].

3.6. Câu hỏi ôn tập và thực hành

Câu 1. Hãy trình bày về khái niệm phương pháp giấu tin trong âm thanh? Hãy nêu các yêu cầu đối với kỹ thuật giấu tin trong âm thanh?

Câu 2. Hãy liệt kê các phương pháp phân loại giấu tin trong âm thanh?

Câu 3. Hãy trình bày phương pháp giấu tin trong âm thanh sử dụng kỹ thuật LSB?

Câu 4. Hãy trình bày khái niệm về mã hóa pha trong âm thanh? Hãy nêu ưu điểm và nhược điểm của kỹ thuật mã hóa pha?

Câu 5. Hãy trình bày về quy trình mã hóa pha trong âm thanh?

Câu 6. Hãy trình bày về phương pháp giấu tin trong âm thanh sử dụng kỹ thuật điều chỉnh tỷ lệ thời gian?

Câu 7. Hãy trình bày về phương pháp giấu tin trong âm thanh dựa vào đặc trưng quan trọng nhất?

Câu 8. Hãy trình bày khái niệm về phương pháp trải phổ? Hãy trình bày về quy trình trải phổ?

Câu 9. Hãy trình bày về phương pháp trải phổ nhảy tần?

Câu 10. Hãy trình bày về phương pháp trải phổ dãy trực tiếp?

Câu 11. Hãy trình bày về phương pháp mã hóa tiếng vang?

Câu 12. Hãy trình bày về 3 ứng dụng của giấu tin trong âm thanh trong thực tế?

Câu 13. Cho tin cần giấu: “Các kỹ thuật giấu tin” và một file âm thanh kỳ (tự chọn). Bằng ngôn ngữ lập trình [33] hãy thực hiện các yêu cầu sau:

a) Trích xuất từ file âm thanh ban đầu đoạn phase đầu tiên của nó và biểu diễn chúng dưới dạng tín hiệu sóng.

b) Thực hiện giấu tin trong âm thanh sử dụng phương pháp mã hóa phase. Hãy xuất ra màn hình các kết quả theo từng bước trong quy trình giấu tin được trình bày trong thuật toán.
c) So sánh tín hiệu sóng của âm thanh ban đầu và âm thanh đã giấu tin.

Câu 14. Cho tin cần giấu: "Các kỹ thuật giấu tin" và một file âm thanh kỳ (tự chọn). Bằng ngôn ngữ lập trình [33] hãy thực hiện các yêu cầu sau:

a) Thực hiện giấu tin vào file âm thanh sử dụng phương pháp tiếng vang với độ trễ để giấu bit 0 là 150, độ trễ để giấu bit 1 là 200.
b) Tính giá trị của cepstrum và tương quan (autocorrelation cepstrum).
c) Thực hiện tách tin theo giá trị cepstrum tìm được.

Câu 14. Cho tin cần giấu: "Các kỹ thuật giấu tin" và một file âm thanh kỳ (tự chọn). Bằng ngôn ngữ lập trình [33] hãy thực hiện các yêu cầu sau:

a) Thực hiện giấu tin vào file âm thanh sử dụng phương pháp tiếng vang với độ trễ để giấu bit 0 là 150, độ trễ để giấu bit 1 là 200.
b) Tính giá trị của cepstrum và cepstrum tương quan (autocorrelation cepstrum).
c) Thực hiện tách tin theo giá trị cepstrum tìm được.

Câu 15. Cho tin cần giấu có chiều dài 8 bit. Mã giả ngẫu nhiên được tạo ra có tần số cao hơn 4 lần so với tín hiệu tin cần giấu.

a) Hãy biểu diễn bit của tin giấu, mã giả và mã sau khi điều chế bằng phương pháp trải phổ dãy trực tiếp.
b) Hãy biểu diễn biểu đồ phổ của tin giấu, mã giả, mã sau điều chế bằng phương pháp trải phổ dãy trực tiếp.
c) Thực hiện tách tin theo giá trị cepstrum tìm được.

Câu 16. Cho tin cần giấu: "M" và một file âm thanh kỳ (tự chọn). Hãy thực hiện các nội dung sau:

a) Thực hiện giấu tin M vào file âm thanh bằng kỹ thuật LSB.
b) Thực hiện tấn công vào file âm thanh đã được giấu tin bằng kỹ thuật nén âm thanh.
c) Thực hiện tấn công vào file âm thanh đã được giấu tin bằng kỹ thuật cộng nhiễu.
d) Thực hiện tấn công vào file âm thanh đã được giấu tin bằng kỹ thuật biến đổi A/D, D/A

CHƯƠNG 4: GIẤU TIN TRONG VIDEO

4.1. Tổng quan về giấu tin trong video

4.1.1. Các đặc trưng của 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. Con người có thể đo được tốc độ khung hình được hiển thị trong mỗi giây. Vì mỗi khung hình là một ảnh kỹ thuật số bao gồm ma trận các điểm ảnh nên nếu nó có chiều rộng *W* và chiều cao *H* thì kích thước khung hình là *W* x *H* điểm ảnh. Trong video mỗi điểm ảnh chỉ có một thuộc tính màu sắc của chúng. Màu sắc của một điểm ảnh được biểu diễn bởi một giá trị các bit cố định. Để hiểu rõ hơn về các thành phần trong video và mối quan hệ giữa chúng, hãy xét ví dụ sau đây: Giả sử video có thể có thời gian (*T*) 1 giờ (3600 giây), kích thước khung hình 640 x 480 (*W* x *H*) ở độ sâu màu 24 bit và tỷ lệ khung hình 25 fps (số khung hình được hiển thị trong 1 giây). Các đặc trưng của một số tham số được tính như sau [10, 14, 24]:

- Điểm ảnh của mỗi khung hình = 640 x 480 = 307200
- Bit trên mỗi khung hình = 307200 x 24 = 7372800 = 7,3728 MB
- Tỷ lệ bit (*BR*) = 7,3728 x 25 = 184,32 Mb / giây
- Kích thước video (*VS*) = 184 Mb /giây x 3600 giây = 663552 Mb = 23,04 MB/giờ

Dựa trên ví dụ ở trên có thể thấy hai thành phần quan trọng nhất quyết định đến tính chất của video là tỷ lệ bit và kích thước video.

4.1.2. Một số định dạng video

Hiện nay các định dạng và chuẩn video đã được phát triển rất phong phú và đa dạng. Dưới đây là một số định dạng và chuẩn của video đang được sử dụng phổ biến hiện nay [25]:

- **MPEG:** Moving Picture Experts Group (MPEG) – "Nhóm các chuyên gia hình ảnh động" là một nhóm các quy tắc hoạt động được thành lập bởi ISO và IEC để thiết lập các tiêu chuẩn cho việc truyền tải âm thanh và video. Công nghệ mới cho phép có nhiều cách để nén dữ liệu video mà vẫn đảm bảo được chất lượng hình ảnh đạt yêu cầu. Một số chuẩn nén MPEG phổ biến như: MJPEG; MPEG-2**;** MPEG-4; Chuẩn H.264. Trong đó chuẩn MPEG-4 là chuẩn cho các ứng dụng đa phương tiện. MPEG-4 là một tiêu chuẩn cho nén ảnh kỹ thuật truyền hình số, các ứng dụng về đồ họa và video tương tác hai chiều (Games, Video conference) và các ứng dụng đa phương tiện tương tác hai chiều (World Wide Web hoặc các ứng dụng nhằm phân phát dữ liệu Video như truyền hình cáp, Internet Video,...). MPEG-4 đã trở thành một tiêu chuẩn công nghệ trong quá trình sản xuất, phân phối và truy cập vào các hệ thống Video.
- **AVI:** Định dạng AVI (Audio Video Interle) là một định dạng số đa phương tiện do Microsoft giới thiệu vào khoảng tháng 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.

- **FLV:** Định dạng FLV (Flash video) là một dạng file nén từ các file video khác để tải lên mạng 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!…
- **H.263:** chuẩn H263 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.
- **WMV:** Định dạng WMV (Windows Media Video) là một định dạng video chứa video được mã hóa theo bộ theo WMV và âm thanh được mã hóa theo codec Windows Media Audio codec.
- **MP4:** Định dạng 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.
- **MOV:** Định dạng 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.
- **H.264 và H.265:** Chuẩn H.264 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 sẻ video phân giải cao. Tệp này có dung lượng thấp nhưng mang lại chất lượng rất cao. H.264 cũng cho chất lượng hình ảnh tốt nhất, kích thước file nhỏ nhất, hỗ trợ DVD và truyền với tốc độ cao so với các chuẩn trước đó. Định dạng H.265 hay còn gọi là HEVC (High Efficiency Video Coding – mã hóa video hiệu suất cao) là một định dạng video mang lại khả năng nén cao gần gấp đôi so với H.264/AVC. Định dạng H.265 giúp giảm băng thông cần thiết để truyền tải phim, đặc biệt là trên các thiết bị di động.

4.1.3. Phân loại kỹ thuật giấu tin trong video

Ba kiểu phân loại chủ yếu của kỹ thuật giấu tin trong video như sau [1, 14, 24]:

- Theo kỹ thuật giấu
  - + Giấu thông tin trong miền hệ số.
  - + Giấu thông tin trong mặt phẳng bit.
  - + Giấu thông tin vào sự thay đổi khung cảnh.
  - + Giấu thông tin vào hệ số khác biệt năng lượng.
  - + Giấu thông tin trong video chuẩn H.264.
  - + Giấu thông tin trong video chuẩn H.265.
- Theo miền giấu
  - + Giấu thông tin trên miền hình ảnh của video.
  - + Giấu thông tin trên miền âm thanh của video.
- Theo mục đích

+ Thủy vân số:
    - Giấu thông tin trong miền hệ số.
    - Giấu tin trong miền nén.
+ Giấu tin mật:
    - Giấu thông tin trong mặt phẳng bit.

Trên đây, giáo trình đã liệt kê về một số thuật toán và phương pháp giấu tin trong video. Độc giả quan tâm đến các thuật toán này cũng như cách thức cầu hình và cài đặt chúng bằng ngôn ngữ lập trình có thể tham khảo tại tài liệu [35].

4.2. Giấu tin trong video dựa trên miền nén

Trong phần 4.1.3 giáo trình đã trình bày tổng quát về một số kỹ thuật giấu tin đang được sử dụng để giấu tin vào video. Đây là một số thuật toán và phương pháp tương đối phổ biến về mức độ ứng dụng và độ hiệu quả. Tiếp theo, giáo trình sẽ đi vào trình bày chi tiết một số thuật toán và kỹ thuật giấu tin này.

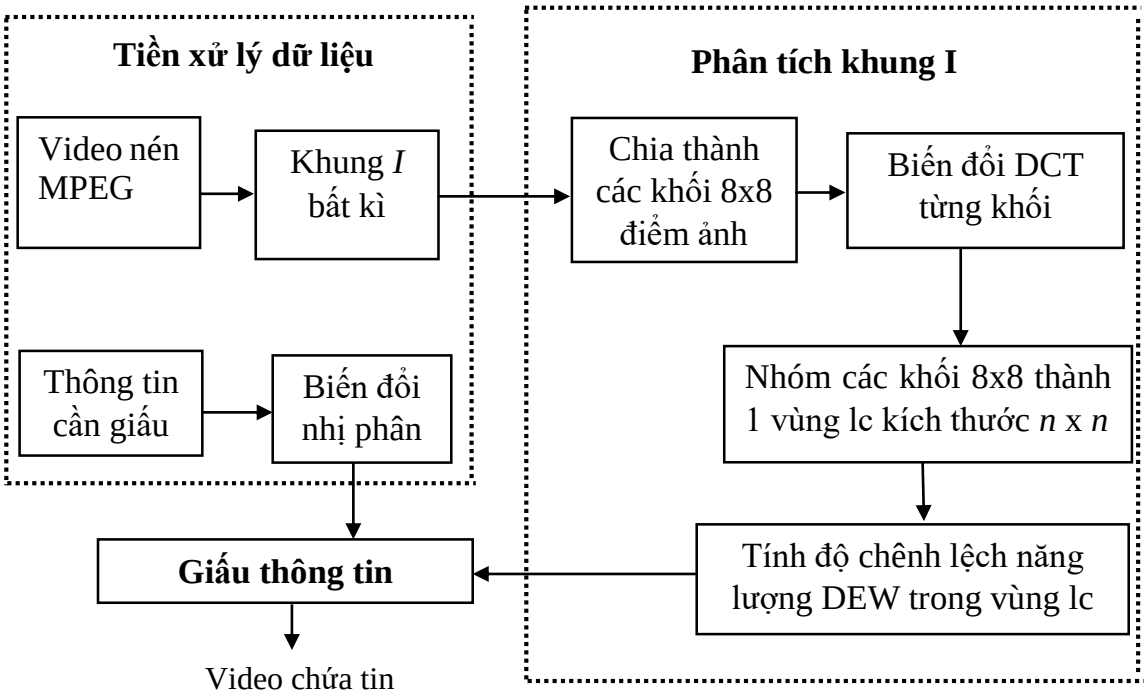
4.2.1. Phương pháp giấu trong miền video nén dựa trên sự khác biệt năng lượng

a) Tổng quan

Các kỹ thuật nhúng thủy vân dựa trên mối tương quan có lợi thế là có thể lấy thủy vân ra được từ việc giải mã các luồng video. Tuy nhiên để nhúng hoặc phát hiện một thủy vân dựa trên mối tương quan thì giải mã MPEG là điều bắt buộc. Mặc dù vậy, trong thực tế việc giải mã các video theo chuẩn MPEG rất mất thời gian và đòi hỏi quá trình tính toán phức tạp. Ngoài ra, như đã biết: việc giấu tin vào các hệ số DCT thấp có ưu điểm là không gây ra hiệu ứng nhiễu mạnh trên hình ảnh hoặc video khi thực hiện giấu tin. Tuy nhiên, việc giấu tin hoàn toàn vào các hệ số DCT thấp có thể dẫn đến việc giấu tin không an toàn, vì những kẻ tấn công có thể phát hiện ra mẫu giấu tin và loại bỏ nó. Bởi vậy giấu tin dựa trên sự khác biệt năng lượng (Difference Energy Watermarking- DEW) được phát triển để giải quyết các vấn đề này. DEW có thể áp dụng trực tiếp trên video nén MPEG/JPEG cũng như trên video nguyên thủy. Phương pháp giấu tin dựa trên DEW là một kỹ thuật giấu tin trong video, trong đó thông tin được giấu vào giá trị khác biệt năng lượng giữa hai khung hình liên tiếp của video. Năng lượng được sử dụng để giấu tin là một đại lượng số học, thể hiện độ lớn của các thay đổi trong giá trị của các điểm ảnh giữa các khung hình liên tiếp trong video. Theo đó, trong video, mỗi khung hình được tạo thành từ hàng và cột các điểm ảnh. Mỗi điểm ảnh có giá trị đại diện cho màu sắc và độ sáng tương ứng trong hình ảnh. Sự khác biệt năng lượng trong giải thuật giấu tin là sự khác biệt giữa giá trị điểm ảnh của các khung hình liên tiếp trong video. Các thay đổi về giá trị điểm ảnh có thể được thêm vào hoặc trừ đi để giấu tin mà không làm ảnh hưởng đáng kể đến chất lượng của video. Theo đó, sự khác biệt năng lượng được tính bằng cách lấy giá trị tổng các năng lượng trong khung hình hiện tại trừ đi giá trị tổng các năng lượng trong khung hình trước đó. Nếu giá trị khác biệt năng lượng lớn hơn một ngưỡng xác định, thông tin giấu sẽ được nhúng vào video. Sử dụng giấu tin dựa trên DEW cho phép giấu thông tin một cách khá hiệu quả và bảo vệ thông tin giấu trước các

kỹ thuật tấn công bằng phương pháp thống kê. Ngoài ra, việc giấu tin vào các vùng có độ chênh lệch năng lượng thấp cũng giúp giảm hiệu ứng nhiễu trên hình ảnh hoặc video khi thực hiện giấu tin, đồng thời cũng tăng tính bền vững của thông tin giấu tin trong trường hợp ảnh hoặc video bị nén hoặc truyền qua kênh mạng không ổn định.

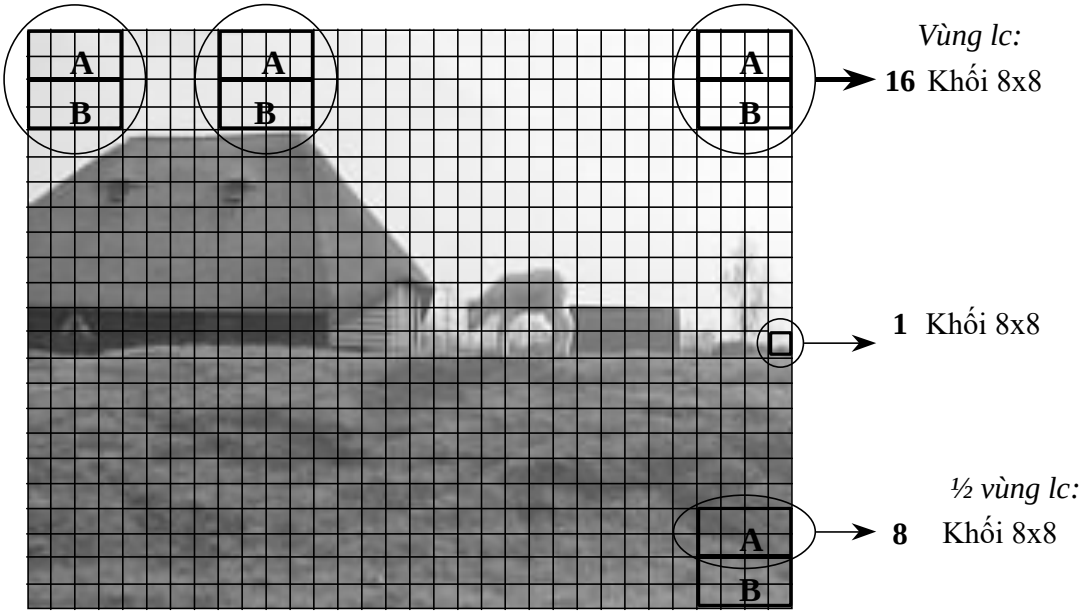
b) Quy trình giấu tin



Hình 4.1. Sơ đồ tổng quát phương pháp giấu tin trong miền video nén dựa bằng DEW

Từ sơ đồ 4.1 có thể thấy, giấu tin trong video theo phương pháp DEW bao gồm các bước sau [1, 24]:

- **Bước 1: Tiền xử lý dữ liệu**. Với 2 thông tin đầu vào là video input và thông tin mật.
  + Đối với thông tin mật: chuyển thông tin mật thành dạng nhị phân.
  + Đối với video input: tiến hành tách video thành các khung hình (tách khung hình ra khỏi luồng nén). Chọn một khung ảnh bất kì để chuẩn bị giấu thông tin mật. Đối với phương pháp DEW nên chọn khung *I* [24].
- **Bước 2: Phân tích khung hình**. Từ sơ đồ hình 4.1 thấy được các bước tiến hành chính trong việc phân tích và xử lý khung hình như sau:
  + Ảnh được chia thành các khối 8x8 điểm ảnh. Rồi từ đó đưa về hệ số DCT (các khối 8x8 hệ số DCT).
  + Nhóm các khối 8x8 thành một vùng *lc* kích thước *n* x *n*: Lưu ý: Trong trường hợp trên với *n = 16* khối 8x8 được gọi là *lc*-region (khu vực *lc*). Kích thước của vùng này được gắn với giá trị tương ứng trên nhãn. Một khu vực *lc* được chia đều thành hai phần *A, B* mỗi phần tương ứng 8 khối 8x8 DCT. Hình 4.2 mô tả ví dụ về việc chia khối *lc*.

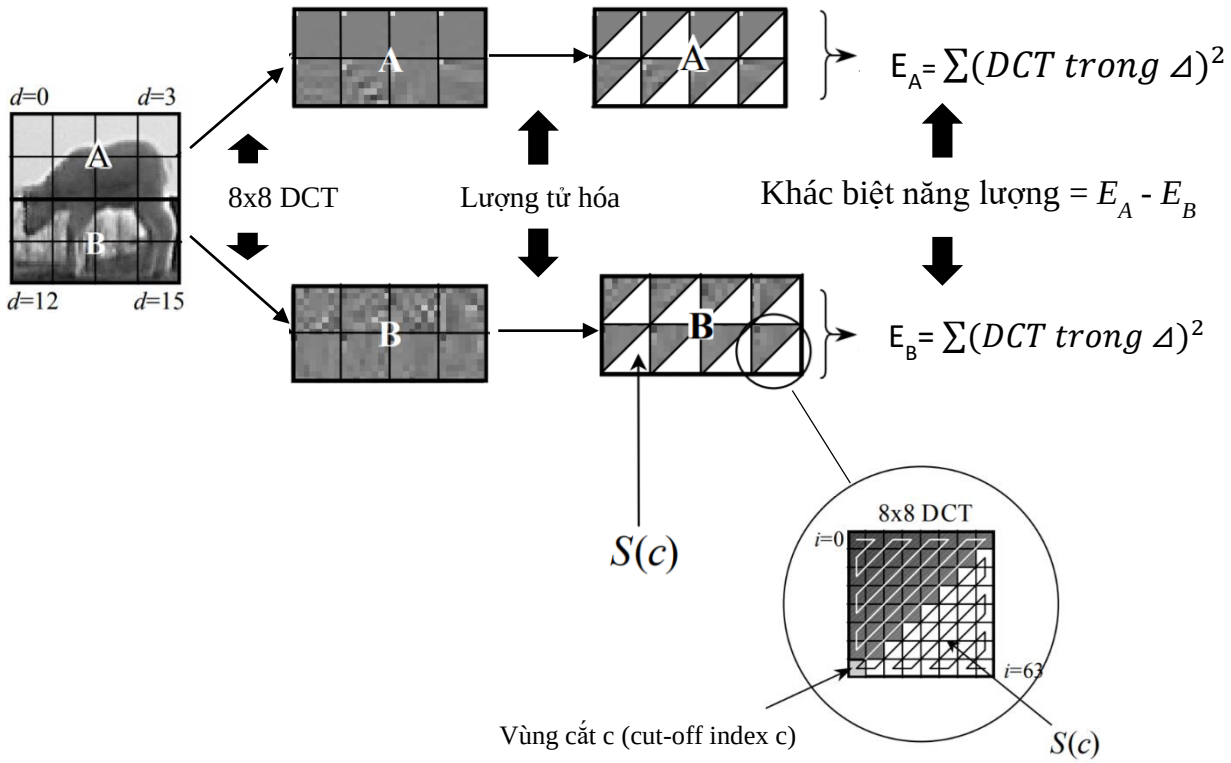


Hình 4.2. Ví dụ về việc chia khối lc

- Tính độ chênh lệch năng lượng trong vùng *lc*: Quy trình tính toán năng lượng trong vùng *lc* được thể hiện như hình 4.3. Theo đó, các thành phần trong quy trình tính toán như sau:

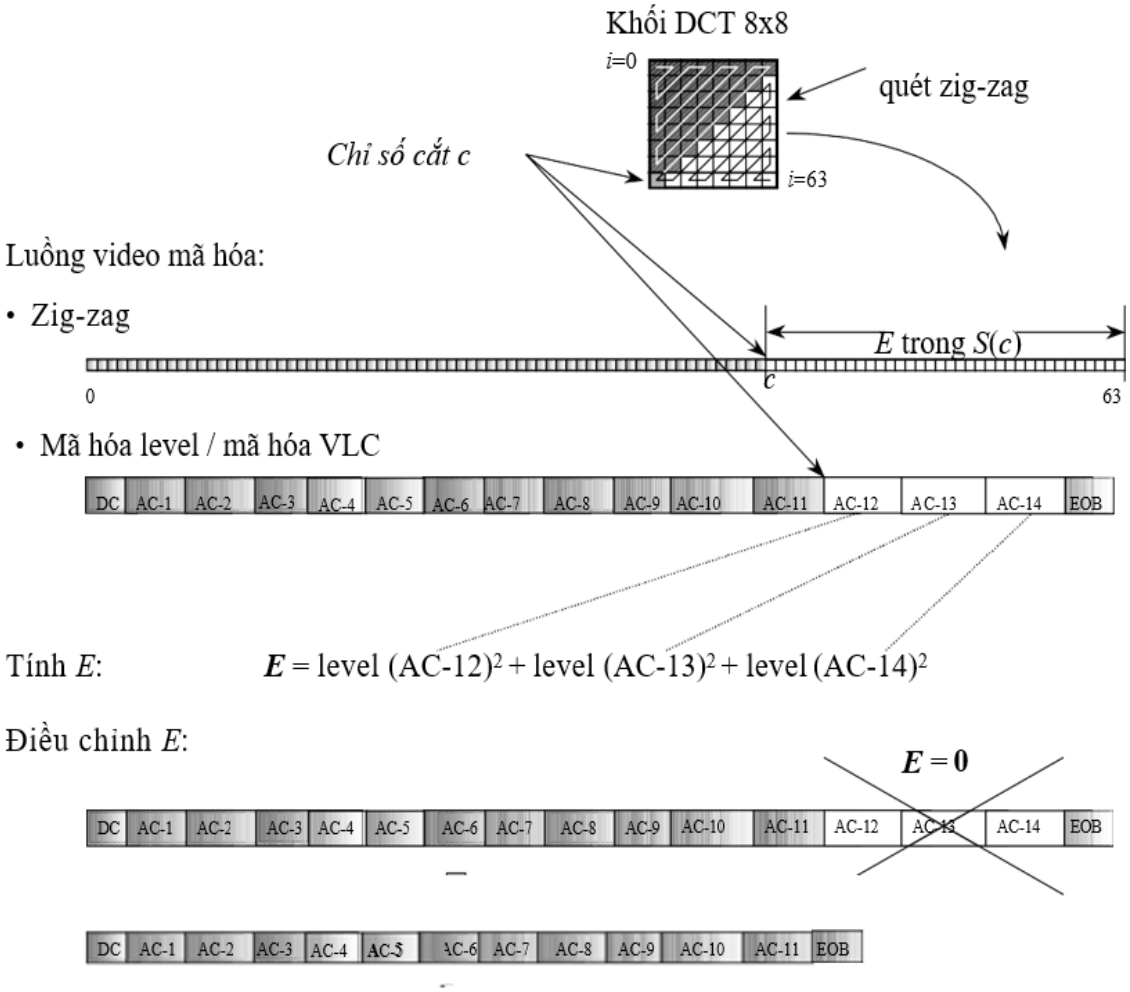
  - E_A năng lượng nửa trên: Năng lượng trong một vùng E_A bằng tổng bình phương của một tập con cụ thể của các hệ số DCT trong vùng E_A này.
  - E_B năng lượng nửa dưới: tính tương tự như E_A
  - D là sự khác biệt năng lượng. Có nhiều phương pháp và cách thức tính toán sự khác biệt năng lượng. Trong giáo trình sẽ lựa chọn cách tính toán sự chênh lệch năng lượng này trên các khu vực hình tam giác. Vì tính toán chênh lệch năng lượng và thay đổi E_A, E_B có thể dễ dàng thực hiện trên luồng nén. Bên cạnh đó, do tất cả các hệ số DCT cần thiết cho tính toán E_A hoặc E_B được đặt ở vị trí thuận tiện ở cuối khối DCT 8x8 theo đường *zig-zag*. Các hệ số này có thể bị đưa về bằng 0 để điều chỉnh năng lượng mà không cần mã hóa lại luồng bằng cách dịch chuyển điểm đánh dấu cuối khối (EOB) về phía hệ số DC. Sự khác biệt được định nghĩa theo công thức 4.1:

$$D = E_A - E_B \tag{4.1}$$



Hình 4.3. Quá trình tính toán năng lượng trong vùng lc

Hình 4.4 minh họa quy trình tính toán *E* trong một khối DCT và thay đổi *E* bằng cách loại bỏ các hệ số DCT nằm ở cuối đường *zig-zag* (nghĩa là các hệ số DCT tần số cao). Từ hình 4.4 thấy được, trong khối các hệ số DCT, hệ số đầu tiên (ở vị trí hàng đầu tiên, cột đầu tiên) được gọi là hệ số *DC*. Hệ số DC biểu thị giá trị trung bình của các điểm ảnh trong khối đầu vào và thường có giá trị lớn hơn các hệ số khác. Các hệ số AC có giá trị thường nhỏ hơn hệ số DC và được sắp xếp theo thứ tự giảm dần của độ quan trọng. Khi đã xác định được các hệ số AC cần giữ lại, EOB được sử dụng để chỉ kết thúc của khối hệ số DCT. EOB được gắn vào cuối các hệ số DCT để chỉ rằng không còn hệ số nào có giá trị khác 0 nữa và kết thúc của khối hệ số DCT đã được đạt đến. Ví dụ nếu có một khối hệ số DCT có 64 hệ số và các hệ số thứ 1, 2, 3, 5, 10 và 20 có giá trị khác 0, các hệ số còn lại bằng 0, thì EOB sẽ được gắn vào sau hệ số thứ 20 để chỉ kết thúc của khối hệ số DCT.



Hình 4.4. Tính toán và điều chỉnh năng lượng trong khối DCT 8x8

+ Tập con này biểu diễn bởi $S(c)$ (hình tam giác trắng trong hình 4.2). Công thức tính năng lượng tại một vùng như sau (xem công thức 4.2):

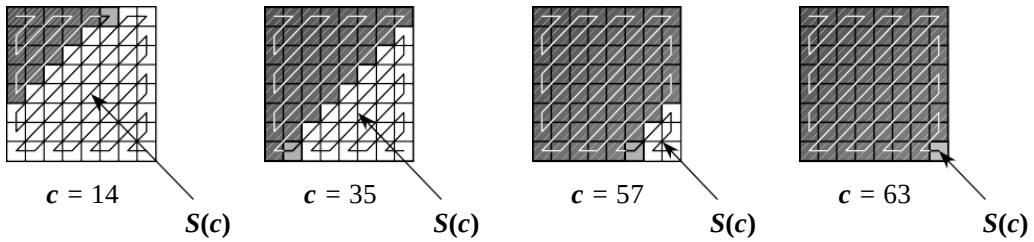
$$E_A(c,n,Q) = \sum_{d=0}^{\frac{n}{2}-1} \sum_{i \in S(c)} ([\theta_{i,d}]_Q)^2 \quad (4.2)$$

Trong đó:

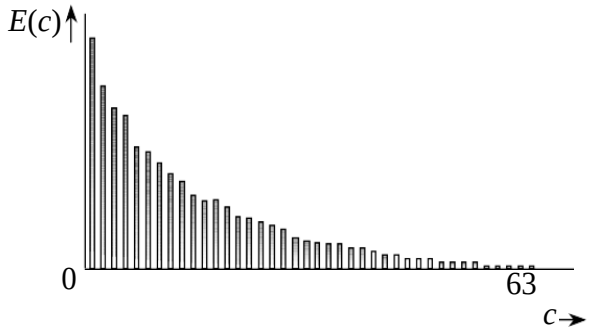
- E_A là năng lượng tại vùng *A*.
- *d* là vị trí khối DCT trong 1 vùng *lc*.
- *i* là vị trí của hệ số DC trong khối DCT.
- $\theta_{i,d}$ (theta) là hệ số DC thứ i của khối DCT thứ *d* của khu vực *A*.
- *Q* là bước lượng tử hóa (xấp xỉ giá trị).

Từ ví dụ trên hình 4.4 cho thấy kích thước của tập hợp con $S(c)$ được xác định bởi phép quét zig-zag và chỉ số *c*. Các hệ số DCT được quét theo hình *zig-zag* được đánh số từ 0 đến 63, trong đó hệ số có chỉ số 0 biểu thị thành phần DC và hệ số có chỉ số 63 là thành phần tần số cao nhất, tập hợp con này bao gồm các hệ số DCT trong các chỉ số c...63 (c >0).

Hình 4.5a được minh họa về các tập hợp con được xác định bằng cách tăng các chỉ số giới hạn. Các năng lượng được xác định bằng thực nghiệm tương ứng được vẽ dưới đây. Hình 4.5b cho thấy việc tăng chỉ số giới hạn làm giảm năng lượng.



(a) Tập con S(c) của các hệ số DCT được xác định bởi chỉ số quét zig-zag và chỉ số cắt



(b) Năng lượng phụ thuộc vào kích thước tập con

Hình 4.5. (a) Ví dụ về tập hợp con và (b) năng lượng cho một số chỉ số giới hạn

- **Bước 3: Giấu thông tin**. Một trong những vấn đề quan trọng trong các hệ thống giấu tin là phải chọn được vùng để giấu thông tin. Theo đó, kỹ thuật giấu tin trong video dựa trên sự khác biệt năng lượng, vùng được chọn để giấu tin thường là các khối 8x8 điểm ảnh, được biến đổi DCT và sử dụng các hệ số DCT ở tần số thấp để làm nơi chứa giấu tin. Các khối 8x8 điểm ảnh này có thể được chọn ngẫu nhiên trên toàn bộ khung hình hoặc theo một mô hình cụ thể. Một số phương pháp chọn vùng thường được sử dụng trong giấu tin trong video dựa trên sự khác biệt năng lượng bao gồm: (1) Phân chia khung hình thành các vùng và chỉ chọn các vùng có độ năng lượng khác biệt lớn so với các vùng lân cận. (2) Chọn các khối nằm ở các vị trí đặc biệt, ví dụ như các khối nằm trên đường biên hoặc ở góc của khung hình. (3) Chọn các khối dựa trên một mô hình thống kê của dữ liệu video, ví dụ chọn các khối nằm trong các khu vực có mật độ nhiễu thấp hoặc các khối ở những vùng có sự thay đổi ít trong khung hình.

Để tính sự chênh lệch năng lượng, quy trình nhúng phải loại bỏ tất cả các hệ số DCT trong tập hợp con $S(c)$ ở vùng lc-của vùng con A hoặc B. Vì việc loại bỏ hệ số dẫn đến biến dạng hình ảnh nên số lượng hệ số DCT bị loại bỏ phải được giảm thiểu. Đồng thời kỹ thuật giấu phải tìm chỉ số giới hạn phù hợp cho từng vùng lc xác định tập con nhỏ nhất $S(c)$ mà năng lượng trong cả hai vùng *lc* của vùng A và B vượt quá chênh lệch năng lượng mong

muốn. Để tìm chỉ số giới hạn xác định tập hợp con mong muốn, trước tiên cần tính năng lượng $E_A(c,n, Q_{jpeg})$ và E_B(c,n, Q_{jpeg}) cho tất cả các chỉ số giới hạn có thể có c = 1...63. Tiếp theo, Nếu D là chênh lệch năng lượng cần thiết để biểu diễn một bit nhãn trong vùng *lc*, thì chỉ số giới hạn c được tìm thấy là chỉ số lớn nhất của các hệ số DCT mà cho năng lượng lớn hơn chênh lệch D cần thiết trong cả hai vùng A và B. Để kiểm soát chất lượng hình ảnh của dữ liệu video được đánh dấu và tránh tình trạng các hệ số DCT tần số thấp quan trọng bị loại bỏ. Yêu cầu chỉ số giới hạn đã chọn luôn lớn hơn c_{min} tối thiểu nhất định. Về mặt toán học, điều này đưa ra biểu thức sau để xác định c như sau (xem công thức 4.3):

$$c(n,Q_{jpeg},D,c_{min}) = \max\{c_{min}, \max\{g\in\{1,63\}|(E_A\ (g,n,\ Q_{jpeg}) > D) \wedge (E_B\ (g,n,\ Q_{jpeg}) > D)\}\} \quad (4.3)$$

Sau khi đã tính toán được sự khác biệt năng lượng giữa các vùng thì người giấu tin sẽ tiến hành giấu thông tin. Nhiệm vụ bây giờ là xác định giá trị của bit tương đương với sự chênh lệch năng lượng D. Bit 0 được xác định là $D > 0$, bit 1 được xác định nghĩa là $D < 0$. Theo đó:

- Nếu bit "0" được giấu, tất cả năng lượng trong vùng cắt c của vùng B được loại bỏ bằng cách đặt hệ số DCT tương ứng bằng 0. Khi đó năng lương D được tính theo công thức 4.4 như sau:

$$D = E_A - E_B = E_A - 0 = +E_A \quad (4.4)$$

- Nếu bit "1" được nhúng, tất cả năng lượng trong vùng cắt c của vùng A được loại bỏ. Khi đó năng lượng D được tính theo công thức 4.5 như sau:

$$D = E_A - E_B = 0 - E_B = -E_B \quad (4.5)$$

Ví dụ dưới đây sẽ thể hiện rõ hơn quy trình giấu thông tin:

- Cần giấu bit $b_0 = 0$. Xét một vùng lc với $n = 2$ (tương ứng với 2 khối DCT).
- Năng lượng khác biệt D = 500.
- Vị trí E_A có năng lượng vượt quá D là i=35.
- Vị trí E_B có năng lượng vượt quá D là i=36.

Từ các thông tin đầu bài cung cấp có thể nhận thấy:

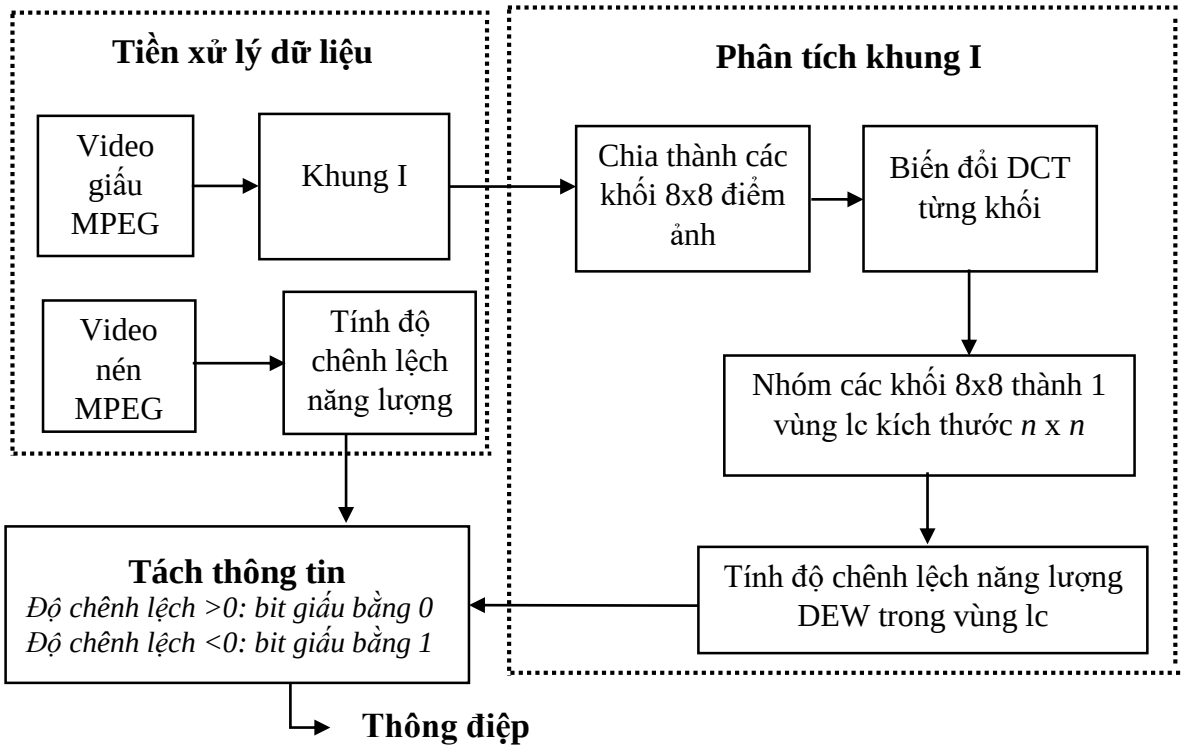
Vì bit nhúng là 0 nên $D > 0$ nên thuật toán phải chọn chỉ số giới hạn c là 35 để có đủ năng lượng ở cả hai tiểu vùng *lc A* và *B*.

Vì bit nhãn phải nhúng là 0, nên chênh lệch năng lượng dương phải được thực thi bằng cách đặt E_B về 0. Điều này được thực hiện bằng cách loại bỏ tất cả các hệ số DCT khác 0 với các chỉ số 35...63 trong tiểu vùng *lc B* (xem hình 4.4). Vậy năng lượng E_B cần phải loại bỏ. Quá trình loại bỏ này được thực hiện theo nguyên tắc loại bỏ các hệ số DCT không bằng 0 từ vị trí thứ 35-63 trong vùng *B*.

c) Quy trình tách tin

Hình 4.6 mô tả quy trình tách tin của kỹ thuật giấu tin trong video dựa trên sự khác

biệt năng lượng.



Hình 4.6. Sơ đồ tổng quát phương pháp tách tin trong miền video nén dựa trên DEW

Từ sơ đồ tách tin trên hình 4.6 thấy được quy trình tách tin sẽ bao gồm các bước sau [1, 24]:

Bước 1: Tiền xử lý dữ liệu. Với 2 thông tin đầu vào là video giấu MPEG và video nén MPEG.

- Đối với video nén MPEG: tiến hành tính độ chênh lệch năng lượng DEW tương tự như bước 2 trong quy trình giấu thông tin.

- Đối với video giấu MPEG: tiến hành tách video thành các khung hình (tách khung hình ra khỏi luồng nén). Chọn một khung ảnh bất kì để chuẩn bị tách thông tin mật. Đối với phương pháp DEW nên chọn khung *I* [24].

Bước 2: Phân tích khung hình. Từ sơ đồ hình 4.6 thấy được các bước tiến hành chính trong việc phân tích và xử lý khung hình được tính toán tương tự như bước phân tích khung hình trong quy trình giấu tin.

Bước 3: Tách thông tin. Tại bước này cần thực hiện các quá trình tính toán sau:

- Xác định vùng chứa thông tin: Tính toán lại năng lượng của từng vùng *lc* và so sánh với năng lượng ban đầu để xác định các vùng đã được giấu thông tin. Các vùng có sự khác biệt năng lượng lớn hơn sẽ được xem là các vùng giấu thông tin. Sau đó sẽ trích xuất

thông tin đã được giấu bằng cách đọc giá trị của các hệ số DCT đã bị thay đổi trong các vùng này.

- Xác định bit giấu:

+ Tìm lại chỉ số giới hạn (*index c*) đã được sử dụng cho vùng lc trong quá trình nhúng.

o Tính năng lượng E_A (c,n, Q_{jpeg}) và E_B (c,n, Q_{jpeg}) cho tất cả các chỉ số giới hạn có thể có c = 1...63.

o Trong *lc*-tiểu vùng *A* hoặc *lc*-tiểu vùng *B*, một số hệ số DCT đã bị loại bỏ trong quá trình nhúng thủy vân, trước tiên, tìm chỉ số lớn nhất của các hệ số DCT mà cho năng lượng lớn hơn ngưỡng $D' \geq D$ trong cả hai tiểu vùng của vùng *lc*.

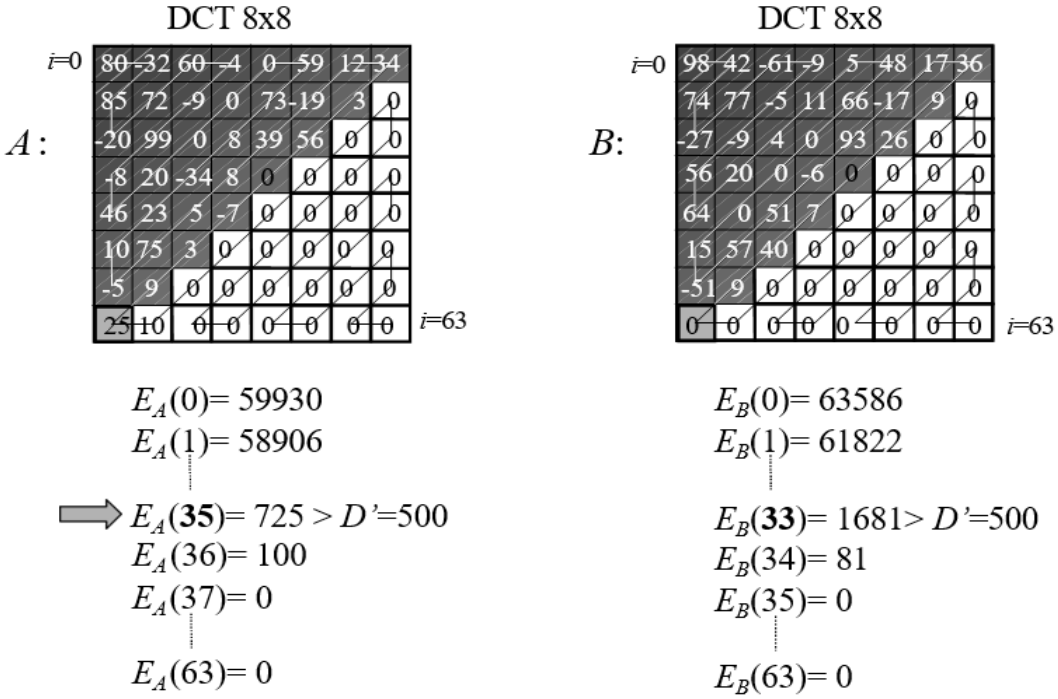
o Chỉ số giới hạn thực sự được sử dụng sau đó được tìm thấy là giá trị lớn nhất của hai số này (xem công thức 4.6).

$$c^{(extract)}(n,Q'_{jpeg},D') = max\{max\{g\in\{1,63\}|(E_A(g,n,Q'_{jpeg}) > D')\},\ max\{g\in\{1,63\}|(E_A(g,n,Q'_{jpeg}) > D')\}\} \quad (4.6)$$

- Tính năng lượng E_A, E_B với chỉ số index c tìm được.
- Tính độ chênh lệch năng lượng $D = E_A - E_B$

+ Nếu $D>0$: bit giấu bằng 0

+ Nếu $D<0$: bit giấu bằng 1



Hình 4.7. Ví dụ về trích xuất bít nhãn b_0 từ vùng lc

Trên hình 4.7 thể hiện một ví dụ về việc trích xuất bit nhãn b_0 từ vùng lc bao gồm *n=2* khối DCT đã được đánh dấu trong hình 4.1. Để trích xuất, *D'=D=500* được sử dụng. Chỉ số giới hạn tối đa mà năng lượng E_A vượt quá *D'=500* là 35, đối với E_B chỉ số giới hạn này là 33. Điều này có nghĩa là thuật toán nhúng thủy vân đã sử dụng chỉ số giới hạn là 35. Chênh lệch năng lượng E_A (35)- E_B (35) = +725. Vì chênh lệch năng lượng là dương nên giá trị 0 được gán cho bit nhãn b_0

d) Nhận xét phương pháp

Nhìn chung kỹ thuật giấu tin trong video dựa trên DEW là kỹ thuật mới, kỹ thuật này về cơ bản đã giải quyết được các nhược điểm mà các phương pháp LSB hay DCT gặp phải. Theo đó phương pháp này có một số ưu điểm sau:

- *Mức độ bảo mật cao cho các thông tin được giấu*: Phương pháp này cho phép giấu tin vào các khu vực ngưỡng độ lớn khác nhau của các khối hình ảnh nén, từ đó giúp tăng tính bí mật của thông tin giấu trong video. Bên cạnh đó, phương pháp có khả năng bảo vệ thông tin nhúng trước các kỹ thuật tấn công như: yêu cầu truy cập trái phép, nén, xoay...

- *Khả năng ứng dụng rộng rãi*: Vì những ưu điểm bảo mật cao nên phương pháp giấu tin miền video nén dựa trên sự khác biệt năng lượng là một phương pháp giấu tin hiệu quả và được sử dụng rộng rãi trong ngành công nghiệp sản xuất và xử lý video.

- *Khả năng chịu lỗi tốt*: Dựa vào cấu trúc của phương pháp giấu tin này, thông tin dễ dàng được phục hồi nếu bị mất dữ liệu hoặc bị lỗi trong quá trình truyền tải. Theo đó, với kỹ thuật giấu này thì thông tin được giấu tin vào video sẽ được phân bố trên nhiều khối hình ảnh và các phần tử khác nhau trong video. Do đó, thông tin giấu tin có thể được phục hồi nếu chỉ một phần nhỏ của video bị mất hoặc bị lỗi.

- *Khả năng tùy chỉnh*: Phương pháp giấu dựa DEW cung cấp khả năng tùy chỉnh độ tin cậy, cho phép người dùng kiểm soát mức độ bảo mật và độ tin cậy cho thông tin giấu vào video. Cụ thể phương pháp này cung cấp cơ chế có thể điều chỉnh ngưỡng năng lượng, kích thước khối, vị trí giấu tin... cho phép quyết định đâu là các điểm ảnh nơi thông tin được giấu tin. Khi ngưỡng năng lượng được nâng cao, độ tin cậy của thông tin giấu tin cũng tăng lên. Và ngược lại, khi ngưỡng được giảm, độ tin cậy cũng giảm.

- *Tốc độ xử lý nhanh*: Phương pháp DEW có tốc độ xử lý nhanh và linh hoạt vì quá trình giấu tin được thực hiện trực tiếp trên dữ liệu video đã nén, không cần giải nén hoặc xử lý trước. Điều này giúp cho phương pháp có tốc độ xử lý nhanh hơn so với khi giấu tin trên video chưa nén. Bên cạnh đó phương pháp này áp dụng kỹ thuật phân tích năng lượng và không tốn nhiều tài nguyên.

Ngoài những ưu điểm được liệt kê ở trên, phương pháp này cũng có một số nhược điểm nhất định như:

- *Độ chính xác ảnh hưởng khi độ sáng và tín hiệu nhiễu trong video thay đổi:* DEW chỉ hoạt động tốt khi các khối hình ảnh của video có độ tương đồng cao với nhau. Nếu các

khối hình ảnh khác nhau quá nhiều, sẽ rất khó để thực hiện nén video và giấu giấu thông tin một cách chính xác.

- *Không chống lại được các kỹ thuật giả mạo video mới*: Các kỹ thuật giả mạo video ngày càng phát triển, làm cho việc trích xuất thông tin trở nên khó khăn và không chính xác.

Có thể thấy rằng nhược điểm của DEW chủ yếu liên quan đến độ tin cậy, tốc độ xử lý, độ chính xác và ổn định. Tuy nhiên, những vấn đề này có thể được khắc phục thông qua việc tối ưu hóa thuật toán và sử dụng các kỹ thuật bổ sung để tăng cường độ tin cậy và ổn định của thuật toán (Embedded Zerotree Wavelet). Chi tiết thuật toán này được mô tả trong tài liệu [24].

4.2.2. Phương pháp giấu trên miền nén của video chất lượng cao

a) Giới thiệu chung

Ngày nay chất lượng video ngày càng được cải thiện với sự hỗ trợ của các chuẩn mã hóa video mới. Các kỹ thuật này không chỉ cho phép nén và tạo ra các video có chất lượng tốt mà còn giảm được dung lượng lưu trữ. Ngoài ra, vấn đề lưu trữ và truyền dữ liệu video qua các kênh truyền thông cũng có nhiều điểm khác biệt so với các cách truyền thống. Một số công nghệ và giải pháp hiện nay yêu cầu thu và phát video phải được thực hiện trong thời gian thực. Do đó, để xác thực được nội dung cũng như bảo vệ được bản quyền tác giả cho các video như vậy đòi hỏi các kỹ thuật giấu tin phải có những cách tiếp cận mới. Để giải quyết các vấn đề này, kỹ thuật giấu tin trên miền nén video chất lượng cao được ra đời. Phương pháp giấu tin trên miền nén của video chất lượng cao hoạt động bằng cách sử dụng phương pháp chèn dữ liệu vào các khung ảnh nén của video. Cụ thể, các thông tin cần giấu sẽ được chia thành các phần rồi giấu vào các khối dữ liệu được nén của video chất lượng cao thông qua các kỹ thuật như chèn thêm bit, ảnh hưởng đến các điểm ảnh hoặc phân phối các giá trị DCT trong khối. Các phần dữ liệu sẽ được chèn vào vị trí nhất định trong các khối DCT, đảm bảo rằng thông tin giấu không ảnh hưởng đến chất lượng video. Để hiểu rõ hơn về quy trình giấu tin và tách tin trong video chất lượng cao dựa trên miền nén, giáo trình sẽ đi vào phân tích và mô tả chúng trong các mục (b) và (c).

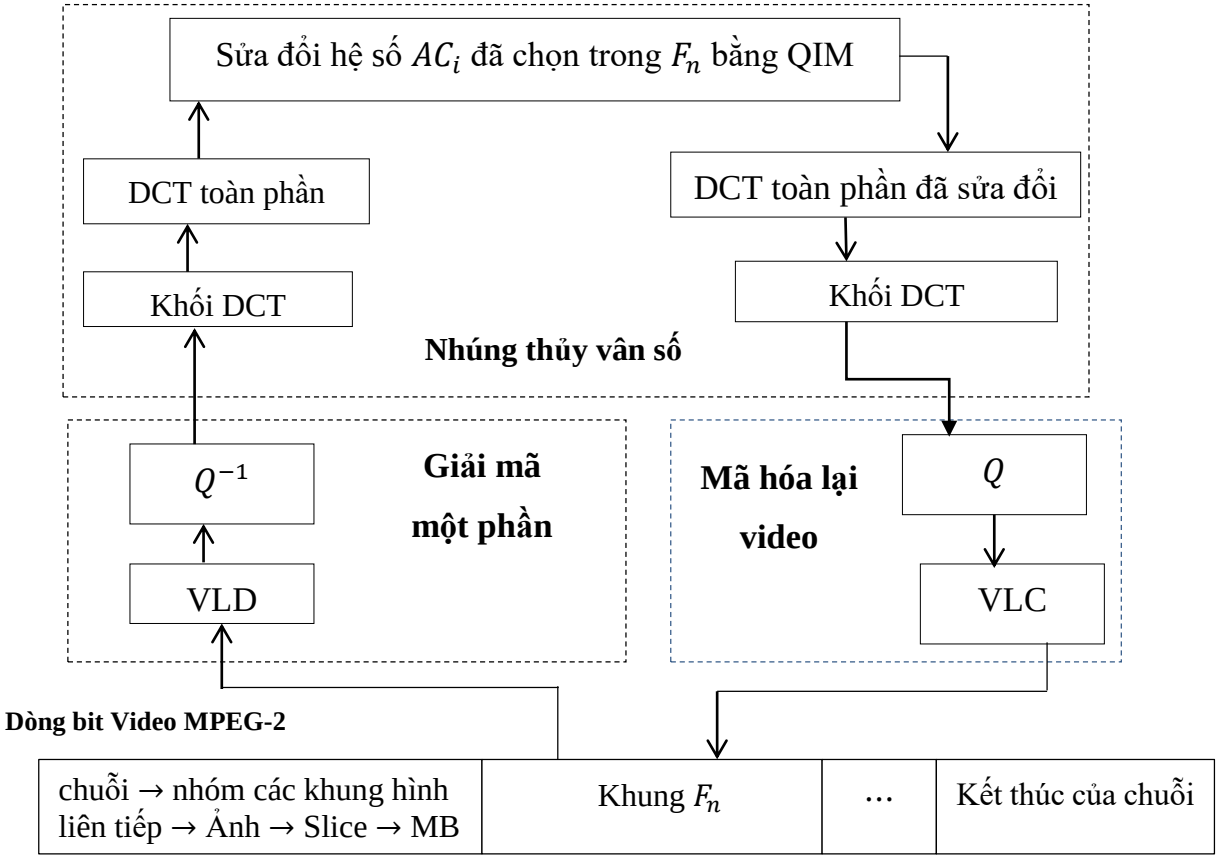
b) Quy trình giấu tin

Từ quy trình giấu tin trong video thể hiện trên hình 4.8 thấy được các bước chính trong kỹ thuật giấu tin trên miền nén của video chất lượng cao như sau [1, 24]:

Bước 1. Lựa chọn khung. Như đã biết, các khung trong video chất lượng cao gồm: khung *I* (intra-frame); Khung *P* (predictive frame) và khung *B*-frame (bi-directional predictive frame). Các khung này đóng vai trò quan trọng trong việc nén và truyền tải video. Trong đó: Khung *I* là khung độc lập, chứa đầy đủ thông tin hình ảnh của một khung hình. Được gọi là khung gốc của video. Khung *I* không phụ thuộc vào bất kỳ khung hình nào khác để tái tạo lại thông tin hình ảnh. Vì vậy, khi một khung *I* được mất đi, video sẽ bị gián đoạn. Khung *I* thường được sử dụng để chuyển đổi giữa các cảnh hoặc đoạn video khác nhau.

Khung *P* là khung dự đoán, được nén bằng cách sử dụng thông tin từ khung trước đó. Điều này giúp giảm dung lượng video và tăng tốc độ truyền tải. Tuy nhiên, để khôi phục lại thông tin hình ảnh thì khung *P* phải được kết hợp với khung *I* hoặc các khung *P* khác. Cuối cùng khung *B* là khung dự đoán hai chiều, được nén bằng cách sử dụng thông tin từ khung trước và sau nó. Khung *B* giúp giảm dung lượng video hơn nữa so với khung *P*, nhưng cũng đòi hỏi nhiều tài nguyên hơn khi giải mã.

Từ những phân tích và mô tả về các khung trong video chất lượng cao có thể thấy được rằng: để quá trình giấu tin và tách tin được diễn ra thuận lợi, an toàn và hiệu quả thì người giấu tin nên chọn khung *I* vì khung *I* là khung cơ sở và có thể coi là ảnh gốc, với khung này khi giải mã thì không cần lấy thông tin từ khung khác.



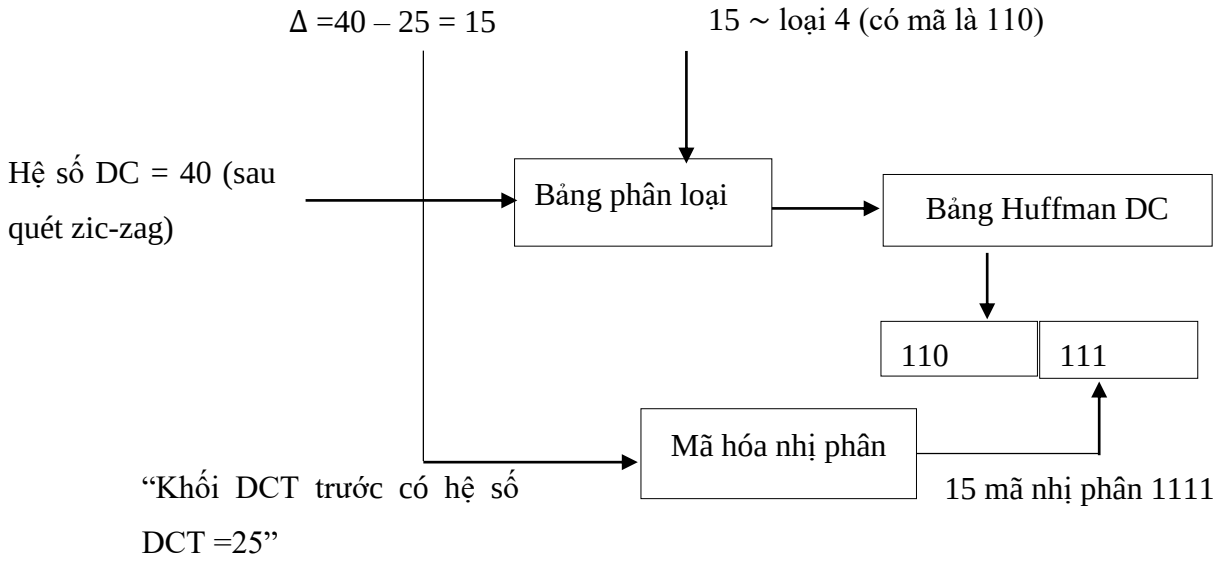
Hình 4.8. Quy trình giấu tin trong nội dung video MPEG -2

Bước 2. Giải mã một phần video. Sử dụng khung đã chọn ở bước 1. Việc giải nén một phần của video sử dụng hai phương pháp chính là VLD (Variable Length Decoding- mã hóa có độ dài biến đổi được) và giải lượng tử hóa. Trong đó:

- *VLD:* các từ mã có tần suất xuất hiện thấp sẽ được mã hoá bằng các từ mã dài, quá trình này được gọi là phương pháp mã hoá từ mã có độ dài thay đổi. Phương pháp này còn được coi là mã hóa Huffman và mã hóa entropy dựa trên khả năng xuất hiện của các biên độ trùng hợp trong một khung ảnh. Theo đó, VLD sẽ thiết lập một từ mã ngắn cho các giá trị

có tần suất xuất hiện cao nhất và từ mã dài cho các giá trị còn lại. Quá trình mã hóa này được tiến hành trên tất cả các thành phần của hệ số DCT. Cụ thể:

+ Với thành phần DC: Giá trị sai lệch hệ số DC sẽ được mã hóa nhờ bảng phân loại và bảng Huffman (dựa vào đặc tính thống kê của tín hiệu). Bảng 4.1 thể hiện giá trị và phân loại của Huffman cho thành phần DC. Các số liệu thống kê trên bảng này sẽ được sử dụng để thực hiện mã hóa entropy thành phần hệ số DC. Hình 4.9 thể hiện một ví dụ về các bước mã hóa entropy thành phần hệ số DC:

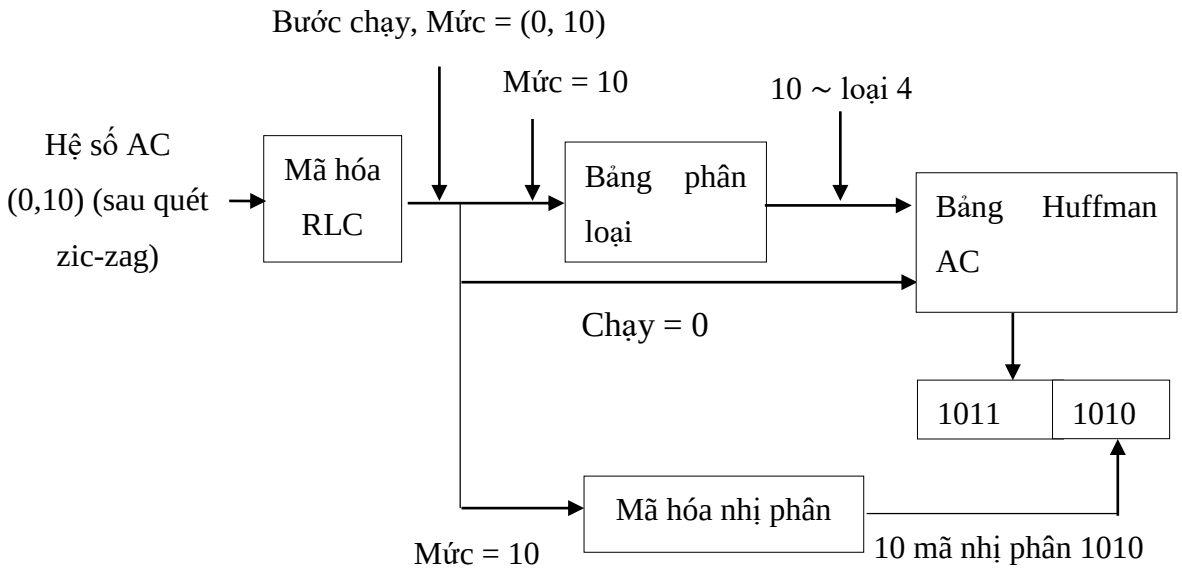


Hình 4.9. Quy trình mã hóa entropy thành phần hệ số DC

Bảng 4.1. Phân loại và bảng Huffman cho thành phần DC

Các hệ số DC sai lệch	**Phân loại**	**Từ mã**
-255…-128; 128…255	8	1111110
-127…-64; 64…127	7	1111 10
-63…-32; 32…63	6	1111 0
-31…-16; 16…31	5	1110
-15…-8; 8…15	4	110
-7…-4; 4…7	3	101
-3; -2; 2; 3	2	01
-1; 1	1	00
0	0	100

+ Với thành phần AC: Hệ số AC cũng được mã hóa nhờ bảng phân loại (giống như DC) và bảng Huffman (nhưng khác DC xem bảng 4.2). Ví dụ về một quy trình mã hóa entropy thành phần hệ số AC được mô tả trong hình 4.10.



Hình 4.10. Quy trình mã hóa entropy thành phần hệ số AC

Bảng 4.2. Huffman các hệ số AC

Bước chạy	**Phân loại**	**Độ dài mã**	**Từ mã**
0	1	2	00
0	2	2	01
0	3	3	100
0	4	4	1011
1	1	4	1100
1	2	6	111001
2	1	5	11011
2	2	8	1111 000
3	1	6	111 010
4	1	6	111 011
5	1	7	1111 010
6	1	7	1111 011
EOB		4	1010

- *Lượng tử hóa:* Mục đích của việc lượng tử hóa là giảm số lượng bit cần để lưu trữ các hệ số biến đổi bằng việc giảm độ chính xác của các hệ số này cho nên lượng tử là quá trình xử lý có mất thông tin. Theo đó, đầu vào ở bước này là 64 hệ số DCT của khối 8x8 sẽ được lượng tử hoá dựa trên một bảng lượng tử gồm 64 phần tử *Q(u, v) với 0≤ u, v≤7*. Nguyên tắc lượng tử là chia các hệ số *F(u, v)* cho các hệ số ở vị trí tương ứng trong bảng lượng tử *Q(u, v)*. Trong chương 2 giáo trình đã trình bày chi tiết về bước lượng tử hóa trong kỹ thuật biến đổi DCT. Bảng lượng tử được xây dựng theo nguyên tắc là mắt người ít cảm nhận được nội dung ở tần số cao và đặc biệt càng kém nhạy với nội dung ở tần số cao của kênh màu. Do đó các hệ số tương ứng với thành phần DC và các thành phần tần số thấp có giá trị lớn nên phải được lượng tử chính xác. Còn các hệ số tương ứng với thành phần tần số AC có giá trị nhỏ nên cho phép sai số.

Bước 3. Giấu thông tin. Dựa trên các mô tả trên hình 4.8 có thể thấy được các kỹ thuật xử lý chính để có thể giấu được thông tin vào khung *I* bao gồm:

- *Giai đoạn 1: Thực hiện tính toán DCT cho toàn khung hình*: Sau khi giải nén một phần video thu được các khối hệ số DCT 8x8 điểm ảnh. Ở giai đoạn này người giấu tin cần thực hiện tính toán DCT cho toàn khung hình từ khối hệ số DCT 8x8 điểm ảnh vừa thu được. Hệ số DCT đầy đủ được tính như sau (xem công thức 4.7): giả sử kích thước khung hình là $LN \times MN$ và kích thước của một khối $B_{i,j}$ là *N*. *L* và *M* số hàng và cột trong hàng tương ứng.

$$FullDCT = \sqrt{\frac{1}{LM}} A_1 . \begin{pmatrix} B_{0,0} & B_{0,1} & \cdots & B_{0,M-1} \\ B_{1,0} & B_{0,2} & \cdots & B_{1,M-1} \\ \vdots & \vdots & \vdots & \vdots \\ B_{L-1,0} & B_{L-1,1} & \cdots & B_{L-1,M-1} \end{pmatrix} . A_2^T \quad (4.7)$$

Trong đó:

$LN \times MN$: kích thước khung hình;

L và *M* số hàng và cột trong hàng tương ứng;

N kích thước của một khối $B_{i,j}$. $B_{i,j}$ là ma trận với $N \times N$ yếu tố và đại diện cho tập hợp các hệ số DCT cho khoanh vùng.

A_1và A_2 là các ma trận vuông với $LN \times LN$ và $MN \times MN$ kích thước tương ứng và được định nghĩa theo công thức 4.8 và 4.9:

$$A_1 = \begin{cases} \sqrt{\frac{1}{2}} a(u,i), & u = 0, \ \ i \ mod \ N \ \neq 0 \\ \sqrt{2} a(u,i), & u \neq 0, \ \ i \ mod \ N = 0 \\ a(u,i), & còn \ lại \end{cases} \quad (4.8)$$

$$A_2 = \begin{cases} \sqrt{\frac{1}{2}} a(v,j), & v = 0, \ \ j \ mod \ N \ \neq 0 \\ \sqrt{2} a(v,j), & v \neq 0, \ \ j \ mod \ N = 0 \\ a(v,j), & còn \ lại \end{cases} \quad (4.9)$$

Trong đó:

$$a(u,i) = \cos\left(\frac{(2i+1)u\pi}{2LN}\right)u, \;\; i = 0,1,\dots,LN-1$$

$$a(v,j) = \cos\left(\frac{(2j+1)v\pi}{2MN}\right)v, \;\; j = 0,1,\dots,MN-1$$

- *Giai đoạn 2: Điều chỉnh chỉ số lượng tử hóa*: Sử dụng phương pháp điều chỉnh chỉ số lượng tử hóa (Quantization Index Modulation -QIM) để giấu thông tin vào các hệ số tần số thấp của hệ số DCT toàn khung hình. Phương pháp QIM do Chen và Wornell giới thiệu là một kỹ thuật giấu tin trong đó dữ liệu được ẩn trong tín hiệu số bằng cách thay đổi các giá trị lượng tử hóa của tín hiệu [24]. QIM sử dụng quy trình lượng tử hóa để chuyển đổi tín hiệu liên tục thành tín hiệu số. Trong quá trình này, tín hiệu liên tục được chia thành các mức lượng tử, mỗi mức tương ứng với một giá trị số nguyên. Sau đó, dữ liệu cần giấu được giấu trong tín hiệu số bằng cách thay đổi giá trị của các mức lượng tử. Việc thay đổi này phải được thực hiện sao cho không làm giảm chất lượng tín hiệu gốc. Trong QIM, dữ liệu được giấu bằng cách thay đổi giá trị của các mức lượng tử theo một quy luật được xác định trước. Quy luật này phải được giữ bí mật để đảm bảo an toàn của dữ liệu giấu tin. Để thực hiện được nhiệm này cần thực hiện các quá trình tính kích thước bước *Q*. Trong thực tế, quá trình tính toàn kích thước bước *Q* áp dụng công thức 4.10:

$$\Delta = 2\max(|\alpha|,|\beta|) = 2max\left(2\left|\sum_{j=1}^{n}\frac{|X_j-\mu|}{X^2_{2n,1-\frac{\tau}{2}}}\right|, 2\left|\sum_{j=1}^{n}\frac{|X_j-\mu|}{X^2_{2n,\frac{\tau}{2}}}\right|\right) \qquad (4.10)$$

Trong đó:

α, β: khoảng tin cậy

μ: tham số vị trí (là giá trị trung bình của biểu đồ)

τ: tỷ lệ bit lỗi BER

X: chuỗi các biểu đồ khác biệt

X^2_{2n}: biểu thị định lượng pth của phân bố X^2 với bậc tự do *2n*

- *Giai đoạn 3: Chọn vị trí nhúng:* Các hệ số xung quanh thành phần DC thường có các giá trị lớn, do đó việc sửa đổi chúng làm giảm chất lượng hình ảnh nghiêm trọng. Ngoài ra, các giá trị hệ số gần thành phần DC thì giá trị của chúng sẽ càng khác nhau sau khi mã hóa lại. Do đó, nên lựa chọn các thành phần tần số trung gian làm vị trí nhúng để cân bằng giữa độ bền và chất lượng hình ảnh. Bên cạnh đó do ảnh hưởng của nén MPEG trên video được nhúng tần số trung bình thấp thích hợp cho việc giấu tin.
- *Giai đoạn 4: Giấu thông tin vào hệ số DCT.* Sau khi thiết lập các tham số cho QIM, thông tin được nhúng bằng cách thay thế các hệ số DCT bằng các giá trị được lượng tử hóa (xem hình 4.11). Hình mờ bao gồm một chuỗi nhị phân, $w = \{w_1, w_2, \dots, w_n\}$, trong đó $w_k \in \{0,1\}$ và *n* có nghĩa là độ dài của thông tin cần giấu. $x = \{x_1, x_2, \dots, x_n\}$ được chọn

các hệ số DCT toàn khung của một khung và $y = \{y_1, y_2, \dots, y_n\}$ được sửa đổi hệ số sau khi giấu thông tin. Sử dụng hàm giấu $E = (x, w)$ như công thức 4.11 tạo ra các giá trị thay thế có khoảng cách tối thiểu giữa giá trị gốc và giá trị được sửa đổi:

$$y_k = E(x_k, w_k) = round\left(\frac{x_k}{\Delta}\right)\Delta + d(x_k, w_k) \quad (4.11)$$

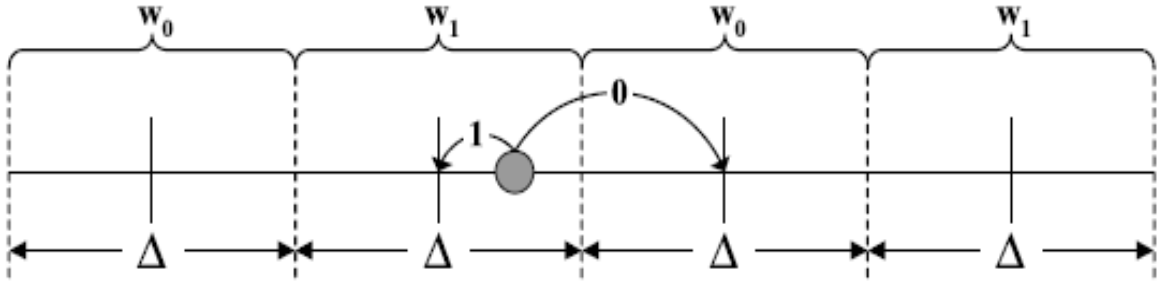
Trong đó:

Δ là kích thước của bước Q

hàm $d(x_k, w_k)$ biểu thị giá trị dithered tương ứng với bit w_k của thông tin mật. Hàm $d(x_k, w_k)$ được tính theo công thức 4.12:

$$d(x_k, w_k) = \begin{cases} \frac{\Delta}{2} \ if(R \ mod \ 2 = 0, \ \ w_k = 0) \ or \ (R \ mod \ 2 = 1, \ w_k = 1) \\ -\frac{\Delta}{2} \ if(R \ mod \ 2 = 0, \ \ w_k = 1) \ or \ (R \ mod \ 2 = 1, \ w_k = 0) \end{cases} \quad (4.12)$$

Trong đó R viết tắt cho $round\left(\frac{x_k}{\Delta}\right)$



Hình 4.11. Thay thế giá trị cho thông tin cần giấu trong QIM

Nguyên tắc giấu thông tin bằng cách sử dụng QIM được mô tả trong hình 4.11 như sau: Giả sử rằng vòng tròn màu xám là giá trị hệ số ban đầu. Nếu một bit thông tin cần giấu là "1" được nhúng vào hệ số này, nó được thay thế cho giá trị trung bình của w_1 là giá trị gần nhất với giá trị hệ số ban đầu. Nếu một bit thông tin cần giấu là "0" được nhúng, nó được thay thế cho giá trị trung bình của w_0 gần nhất.

- *Giai đoạn 5: biến đổi DCT ngược.* Sau khi đã giấu được thông tin bởi QIM bằng cách sử dụng các thông số ở giai đoạn 4 thì các hệ số DCT toàn khung hình đã được sửa đổi và được phân tách thành khối 8×8 điểm ảnh các hệ số DCT. Trong giai đoạn biến đổi DCT ngược chính là cần phải tính toán các khối hệ số DCT nghịch đảo. Quá trình biến đổi DCT ngược được mô tả chi tiết trong chương 2 của giáo trình.

Bước 4: Mã hóa video. Sau khi đã tính toán các khối hệ số DCT ngược, người giấu tin sẽ tiến hành mã hóa video lại sử dụng VLC và giải lượng tử hóa như đã nói ở quá trình giải nén một phần video để tạo các video MPEG-2 chứa thông tin mật. Lưu ý rằng: Quá trình VLC và giải lượng tử ở phía bộ giải mã được thực hiện ngược lại so với các bước biến đổi ở quá trình giải nén video.

c) Quy trình tách tin

Quá trình tách tin trong video dựa trên miền nén video chất lượng cao được tiến hành qua các bước như sau: Trước tiên cần giải nén video bằng phương pháp VLD. Tiếp theo xác định vị trí của các khối hình ảnh trong video mà tin đã được giấu vào dựa trên một số thông tin định dạng video như: kích thước khung hình, số lượng khung hình mỗi giây, ... Sau đó, sử dụng biến đổi DCT ngược cho các khối hình ảnh đã chọn để chuyển đổi lại các hệ số DCT về dạng giá trị điểm ảnh ban đầu. Sau đó tính toán lại các giá trị hệ số DCT ban đầu từ các giá trị lượng tử đã được lưu trữ trong dữ liệu video bằng cách áp dụng quá trình lượng tử hóa ngược. Cuối cùng trích xuất thông tin sử dụng phương pháp QIM. Cụ thể, phương pháp QIM sẽ so sánh giá trị lượng tử của các hệ số DCT với các giá trị lượng tử dự kiến ban đầu (trước khi tin được giấu vào) để xác định giá trị của bit tin đã được giấu vào. Giá trị lượng tử này thường được chọn sao cho nằm giữa giá trị lượng tử của bit 0 và bit 1. Nếu giá trị lượng tử của hệ số DCT lớn hơn giá trị lượng tử dự kiến thì giá trị của bit tin được xác định là 1, ngược lại nếu giá trị lượng tử của hệ số DCT nhỏ hơn giá trị lượng tử dự kiến thì giá trị của bit tin được xác định là 0. Tiếp tục quét các hệ số DCT khác trong các khối hình ảnh còn lại của video để tách ra các giá trị tin ở các vị trí khác. Ví dụ dưới đây sẽ mô tả chi tiết hơn quá trình tách tin: Giả sử giá trị lượng tử của hệ số DCT đã giải nén là Q, giá trị lượng tử dự kiến ban đầu là Q_0, và giá trị tin giấu vào là B (một bit tín chỉ có giá trị 0 hoặc 1). Tính giá trị tuyệt đối của độ chênh lệch giữa giá trị lượng tử của hệ số DCT đã giải nén và giá trị lượng tử dự kiến ban đầu: $|\Delta Q| = |Q - Q_0|$. Nếu giá trị lượng tử của hệ số DCT đã giải nén lớn hơn giá trị lượng tử dự kiến ban đầu, đồng thời giá trị tin giấu vào là 1 ($B = 1$), hoặc giá trị lượng tử của hệ số DCT đã giải nén nhỏ hơn giá trị lượng tử dự kiến ban đầu, đồng thời giá trị tin giấu vào là 0 ($B = 0$) thì giá trị tin được tách ra từ hệ số DCT đã giải nén là 1 ($T = 1$). Nếu giá trị lượng tử của hệ số DCT đã giải nén nhỏ hơn giá trị lượng tử dự kiến ban đầu, đồng thời giá trị tin giấu vào là 1 ($B = 1$), hoặc giá trị lượng tử của hệ số DCT đã giải nén lớn hơn giá trị lượng tử dự kiến ban đầu, đồng thời giá trị tin giấu vào là 0 ($B = 0$), thì giá trị tin được tách ra từ hệ số DCT đã giải nén là 0 ($T = 0$). Công thức tính giá trị tin T từ giá trị lượng tử của hệ số DCT đã giải nén Q, giá trị lượng tử dự kiến ban đầu Q_0, và giá trị tin giấu vào B có thể được biểu diễn như sau (xem công thức 4.13):

$$T = (|Q - Q_0| > 0) \; XOR \; B \tag{4.13}$$

d) Nhận xét về phương pháp

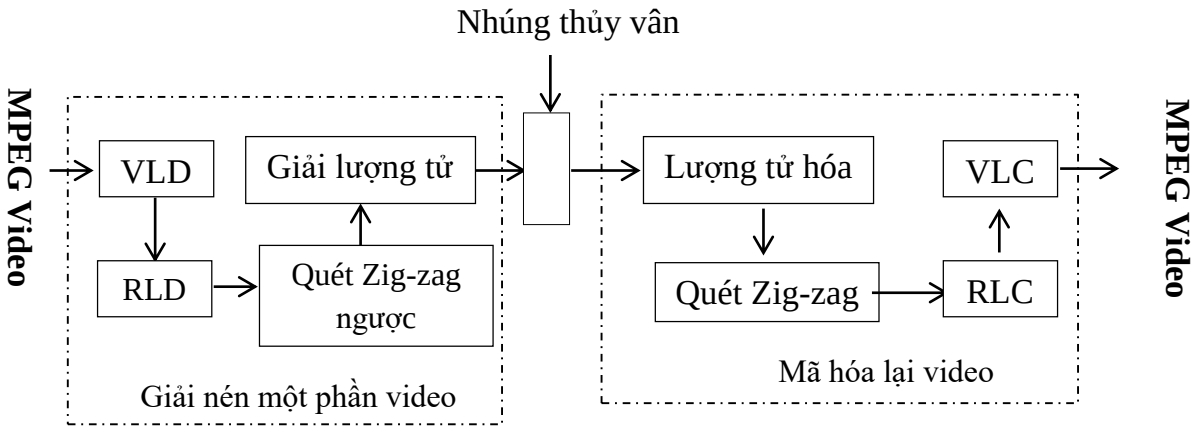
Dựa trên các phân tích và đánh giá về quy trình giấu tin và tách tin bằng phương pháp giấu tin trên miền nén của video chất lượng cao có thể thấy phương pháp này có một số nhược điểm nhất định. Theo đó, quá trình giấu tin có thể làm giảm chất lượng của video, nhất là khi số lượng thông tin giấu tin lớn. Bên cạnh đó, phương pháp này không giấu được nhiều thông tin vì kích thước của các khối dữ liệu nén là giới hạn, do đó, nếu giấu một lượng thông tin lớn sẽ ảnh hưởng đến chất lượng video. Ngoài ra, việc giấu tin trên miền nén của video thường làm tăng độ phức tạp của quá trình giấu tin và tăng thời gian để trích xuất

thông tin. Điều này có thể làm giảm hiệu quả và tốc độ của phương pháp. Mặt khác, kỹ thuật này không chống lại được kỹ thuật tấn công công giải mã dữ liệu. Tấn công giải mã video (video decryption attack) là một kỹ thuật tấn công mà nhằm vào việc phá vỡ các hệ thống mã hóa video để có thể truy cập các thông tin bảo mật hoặc thực hiện các hoạt động xấu khác như sao chép, thay đổi, hoặc phát tán video không được phép. Các tấn công này có thể được thực hiện bằng cách sử dụng các kỹ thuật giải mã ngược, các lỗ hổng bảo mật của hệ thống mã hóa, hoặc các kỹ thuật phá bỏ các chính sách quản lý truy cập.

Ngoài những nhược điểm ở trên thì phương pháp này cũng có nhiều ưu điểm. Đặc biệt phương pháp giấu tin dựa trên miền nén video chất lượng cao có ưu điểm lớn là làm giảm kích thước dữ liệu, do đó, kích thước của video sau khi giấu tin sẽ nhỏ hơn video gốc. Điều này giúp cho việc truyền tải thông tin giấu tin trên mạng trở nên nhanh chóng và tiết kiệm băng thông. Phương pháp cũng cho phép giấu các thông tin bí vào các khối dữ liệu nén của video một cách hiệu quả, mà không gây ra sự thay đổi đáng kể đến chất lượng của video. Đồng thời, do thông tin được giấu trên miền nén nên làm cho việc phát hiện và truy cập thông tin trở nên khó khăn hơn so với việc giấu tin trên video chưa nén. Điều này tăng tính bí mật của thông tin.

4.3. Phương pháp giấu tin trong miền hệ số

a) Tổng quan chung



Hình 4.12. Mô hình tổng quát kỹ thuật giấu tin trong miền hệ số

Từ mô hình tổng quát của kỹ thuật giấu tin trên miền hệ số thể hiện trên hình 4.12 có thể thấy quy trình và nguyên tắc hoạt động của phương pháp này có nhiều điểm tương đồng với kỹ thuật giấu tin trên miền nén của video chất lượng cao. Theo đó, các thành phần chính trong mô hình giấu tin trong miền hệ số bao gồm: *Vật chứa là chuỗi video chuẩn nén MPEG,* luồng video sau đó sẽ được giải nén một phần bằng các bước VLD. Kỹ thuật xử lý thông tin trong VLD đã được trình bày trong mục 4.2.1. *RLC/RLD – Run-level coding/ decoding (mã hóa/ giải mã cấp độ)*: RLC/RLD là hai phương pháp mã hóa và giải mã thông thường được sử dụng để nén và tái tạo các dữ liệu số. Kỹ thuật này sử dụng việc mã hóa các chuỗi các dữ

liệu giống nhau liên tiếp trong một file hoặc một khối hình ảnh/video thay vì lưu trữ mỗi giá trị thành một byte riêng. Trong quá trình mã hóa RLC một chuỗi liên tục các giá trị giống nhau được biểu diễn dưới dạng "số lần xuất hiện liên tiếp" và "giá trị của dữ liệu". Ví dụ: AAABB → 3A2B. Còn RLD là phương pháp giải mã dữ liệu đã được mã hóa bằng RLC. RLD sẽ giải mã dữ liệu đó bằng cách lặp lại từng ký tự tương ứng với giá trị run của nó. Trong kỹ thuật giấu tin trong video dựa trên miền hệ số thì RLC/RLD sẽ thực hiện biến đổi giá trị các thành phần DC và AC trong ma trận một chiều sau VLD. Trong miền run-level, các thành phần hệ số AC khác 0 ở trên được biểu diễn bằng các tập hợp *(run, level).* Trong đó, *run* đại diện cho số các số 0 đứng trước hệ số AC khác 0, còn *level* đại diện cho giá trị của hệ số đó (xem hình 4.9 và 4.10). Các quá trình quét Zig-zag ngược; giải lượng tử; lượng tử hóa; quét Zig-zag; VLC đã đều được định nghĩa ở phần 4.2.1. Trong thực tế để giấu tin vào miền hệ số của video thì có nhiều cách khác nhau. Tiếp theo giáo trình sẽ trình bày 2 cách cơ bản nhất và đang được ứng dụng nhiều hiện nay đó là kỹ thuật sửa đổi hệ số DC (xem phần b) và kỹ thuật sửa đổi hệ số DC, AC và cân bằng độ lệch (xem phần c).

b) Kỹ thuật sửa đổi hệ số DC

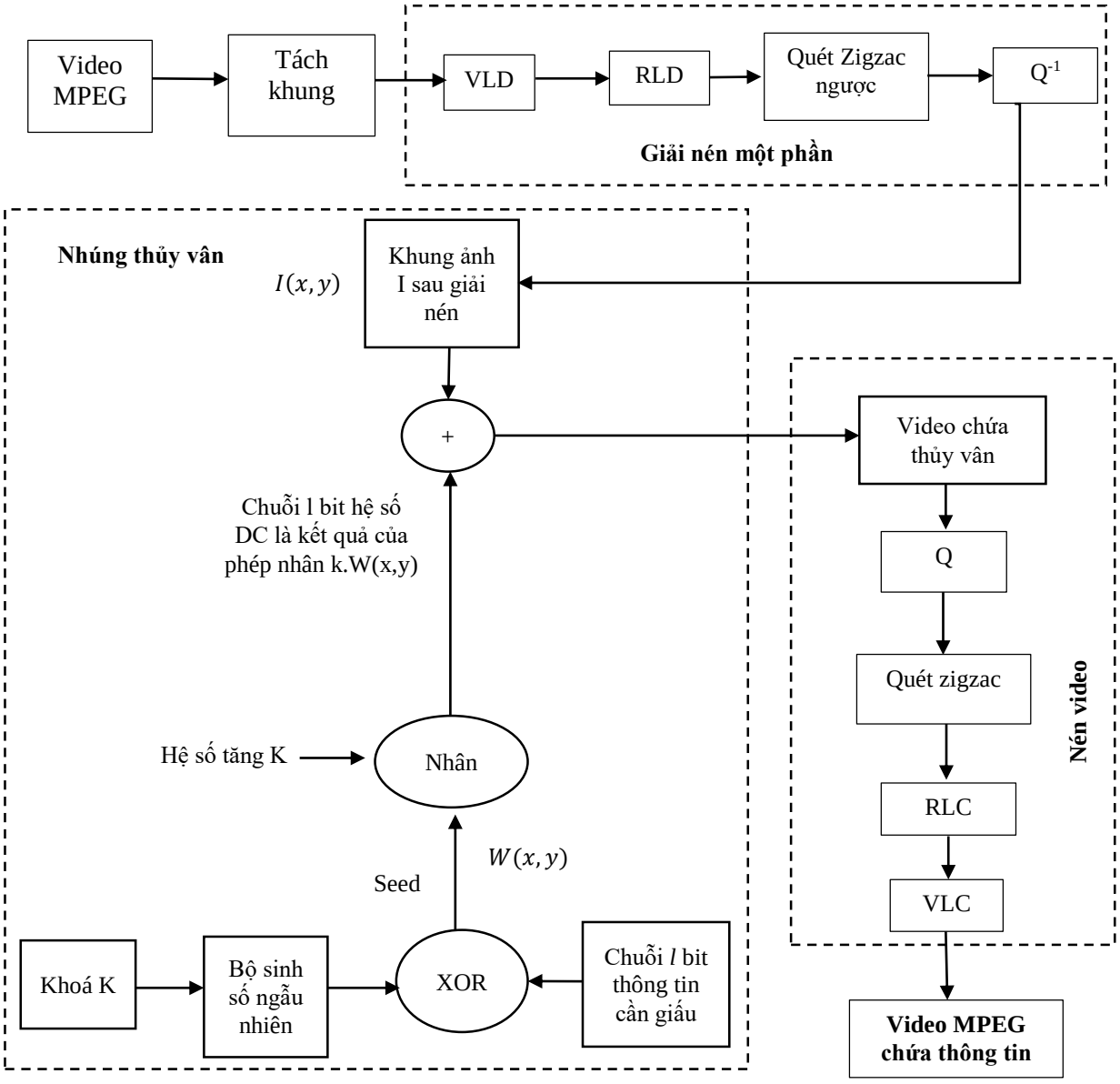
Phương pháp được đề xuất ở đây là thêm một mẫu giả ngẫu nhiên chuyển đổi DCT trực tiếp tới các hệ số DC-DCT của một luồng video nén MPEG. Quá trình giấu tin chỉ tính đến các giá trị luminance Y của khung I. Bởi vì ảnh I được mã hóa mà không có sự so sánh dự đoán từ các ảnh khác. Ảnh I được dùng một cách tuần hoàn để tạo thành điểm tựa cho dòng dữ liệu trong quá trình giải mã. Thị giác của con người lại nhạy cảm với hệ *Y*, ít nhạy cảm hơn so với hệ *U, V*.

Chi tiết quá trình giấu tin trong video trên miền hệ số DC được mô tả trên hình 4.13 như sau: Đầu tiên một mô hình ngẫu nhiên bao gồm các số nguyên (-1, 0, 1) được tạo ra dựa trên một khóa bí mật sử dụng hạt nhân, sổ đăng ký thay đổi tuyến tính hoặc ngẫu nhiên xáo trộn hình ảnh nhị phân. Tiếp theo, với đầu vào là chuỗi l bit thủy vân $b_0 b_1 b_2 \dots b_{l-1}$, ở đây bit 0 được gán giá trị -1, bit 1 được gán giá trị 1. Mỗi giá trị của chuỗi giả ngẫu nhiên được XOR với giá trị tương ứng của chuỗi bit. Một mẫu giả ngẫu nhiên có thể được thêm vào nếu bit trong tin giấu bằng 1, và ảnh phụ I có thể không bị ảnh hưởng nếu bit tin giấu bằng 0. Kết quả thu được sẽ được nhân với một hệ số tăng k. Theo kết quả thực nghiệm [24], hệ số tăng k càng lớn thì tính bền vững của tin mật càng cao. Sau đó, phép biến đổi DCT của khối 8x8 được áp dụng trên mô hình giấu tin thu được từ bước 2 và các hệ số DC được tạo ra sẽ được cộng vào các giá trị DC tương ứng của mỗi khung I. Để nhúng chuỗi l bit thủy vân $b_0 b_1 b_2 \dots b_{l-1}$vào ảnh $I(x, y)$, người giấu tin chia ảnh $I(x, y)$ thành l ảnh nhỏ $I_0 I_1 I_2 \dots I_{l-1}$và thêm một tin giấu cho mỗi ảnh phụ bằng công thức 4.14 như sau:

$$I_W(x, y) = I(x, y) + k.W(x, y) \quad (4.14)$$

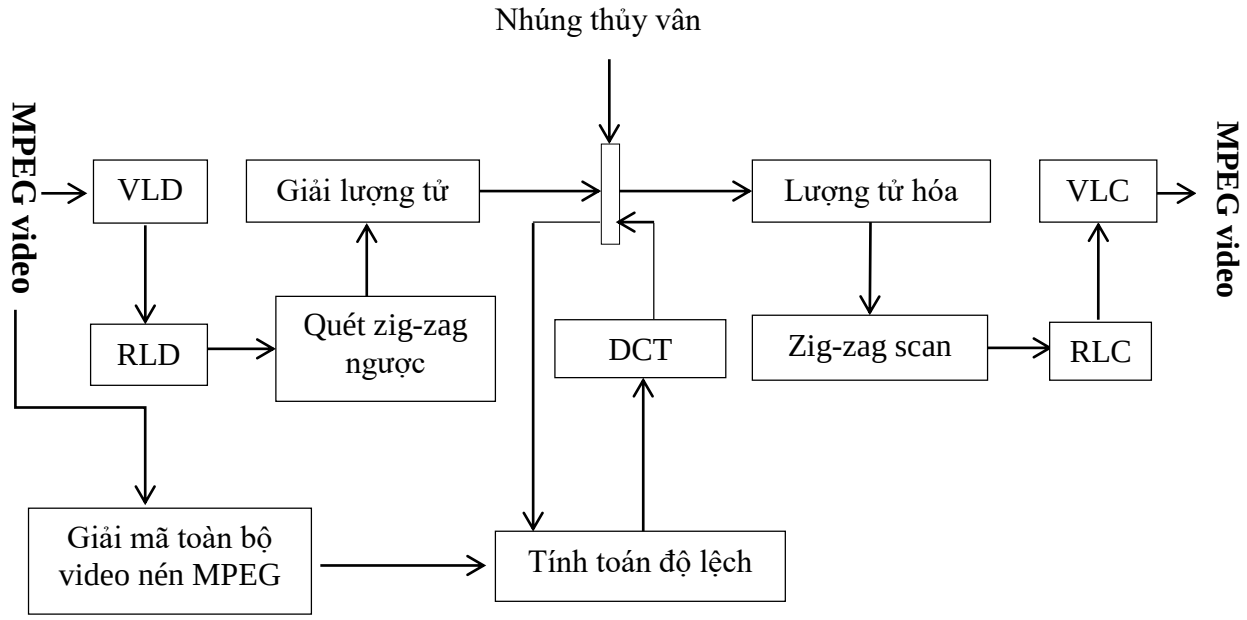
Cuối cùng là nén video. Theo đó, kết quả của quá trình giấu tin sẽ thu được một video chứa thông tin cần giấu. Việc giấu thêm thông tin vào video này sẽ làm dung lượng video tăng lên. Do đó video chứa thủy vân sẽ trải qua thêm quá trình nén lại video để đưa video về

dạng video nén MPEG thông thường. Quá trình này sẽ bao gồm các kỹ thuật xử lý như lượng tử hóa, Quét Zig-zag, RLC, VLC. Chi tiết quá trình này đã được trình bày ở mục 4.2.1 của giáo trình.



Hình 4.13. Sơ đồ giấu tin trong video trên miền hệ số DC

c) Kỹ thuật sửa đổi hệ số DC và AC với hệ số cân bằng độ lệch



Hình 4.14. Quy trình giấu tin trong video dựa trên kỹ thuật sửa đổi hệ số DC và AC với hệ số cân bằng độ lệch

Về cơ bản, ý tưởng của kỹ thuật này giống với ý tưởng của kỹ thuật sửa đổi hệ số DC, nhưng độ phức tạp tăng lên vì phải tính toán độ lệch giữa khung hình dự đoán và khung hình thật của video khi đã được giải nén hoàn toàn. Ở đây phương pháp nhúng được thực hiện không chỉ ở hệ số DC mà còn ở cả hệ số AC của khung *I, P* và *B.* Trong đó khung *I* là khung được mã hóa cho ảnh thực, khung này được tạo ra mà không cần các khung hình khác. Khung *P* là khung được dự đoán thuận từ khung *I* hoặc *B* ngay trước đó. Khung *B* là khung dự đoán vừa thuận vừa nghịch từ khung *I* và *P* lân cận trước và sau khung. Về dung lượng thì khung *I* là lớn nhất, khung *B* nhỏ nhất, do đó thay vì sử dụng khung *P, B* để giảm dung lượng nhớ (theo thời gian) thì dùng khung *I.* Về thứ tự mã hóa thì đầu tiên là khung *I* sau đó là khung *P* cuối cùng là *B.* Đối với mỗi khối video $I_{x,y}(i)$ từ khung *I, P*, hoặc *B*, các bước sau được thực hiện:

- *Tính toán hệ số DC* (xem công thức 4.15)*:*

$$I_{W_{x,y}}(0) = I_{x,y}(0) + W_{x,y}(0) \quad (4.15)$$

Kết quả này thể hiện là khối tin giấu được thêm vào giá trị trung bình của khối video.

- *Tính toán hệ số AC:* Để tính hệ số AC có thể áp dụng công thức 4.16 như sau:

$$I_{W_{x,y}}(i) = I_{x,y}(i) + W_{x,y}(i) \qquad với\ i \neq 0 \quad (4.16)$$

Quá trình này được lặp lại cho tới khi toàn bộ hệ số AC của khối video đã được xử lý. Để hạn chế số lượng bit tăng lên sau khi giấu tin, kích thước Sz_I của VLC $I_{x,y}(i)$ và kích thước Sz_{I_W} của VLC $Iw_{x,y}(i)$ được xác định bằng cách sử dụng các bảng VLC-B.14 và B.15

của tiêu chuẩn MPEG-2 (xem bảng 4.3). Nếu kích thước của VLC mã hóa các hệ số DCT nhỏ hơn hoặc bằng kích thước của VLC hiện tại thì VLC hiện tại được thay thế. Nếu không, VLC sẽ không bị ảnh hưởng. Điều này có nghĩa là hệ số DCT $I_{x,y}(i)$ được tính theo cách sau (xem công thức 4.17):

Nếu $Sz_{I_W} \leq Sz_I$ thì $I_{W_{x,y}}(i) = I_{x,y}(i) + W_{x,y}(i)$; $else\ I_{W_{x,y}}(i) = I_{x,y}(i)$ (4.17)

Quá trình này được lặp lại cho tới khi toàn bộ hệ số AC của video khối đã được thực thi.

Bảng 4.3. Bảng giá trị VLC B-14 và B-15 của chuẩn MPEG

Mã chiều dài thay đổi VLC	VLC size	Run	Level	Cấp độ của LSB
0010 0110 s 0010 0001s	8+1 8+1	0 0	5 6	1 0
0000 0001 1101 s 0000 0001 1000 s	12+1 12+1	0 0	8 9	0 1
0000 0000 1101 0 s 0000 0000 1100 1 s	13+1 13+1	0 0	12 13	0 1
0000 0000 0111 11 s 0000 0000 0111 10 s	14+1 14+1	0 0	16 17	0 1
0000 0000 0011 101 s 0000 0000 0011 100 s	15+1 15+1	1 1	10 11	0 1
0000 0000 0001 0011 s 0000 0000 0001 0010 s	16+1 16+1	1 1	15 16	1 0

- *Hệ số cân bằng độ lệch:* Trong một luồng video MPEG, sự phỏng đoán từ các khung ảnh trước được sử dụng để xây dựng lại khung ảnh thật nhằm mục đích tham khảo cho sự phỏng đoán trong tương lai. Sự suy giảm chất lượng gây ra bởi thủy vân có thể lan rộng theo cả thời gian và không gian. Vì tất cả các khung trong video đều được nhúng thủy vân, thủy vân trong khung trước và khung hiện tại có thể chồng lên nhau. Vì vậy, một tín hiệu cân bằng lệch *Dr* phải được thêm vào. Tín hiệu này cần phải bằng với sai khác giữa sự phỏng đoán từ luồng bit không nhúng thủy vân và có nhúng thủy vân. Công thức tính toán hệ số DCT biến đổi thành (xem công thức 4.18):

$$I_{W_{x,y}}(i) = I_{x,y}(i) + W_{x,y}(i) + Dr_{x,y}(i) \qquad với \quad i \neq 0 \tag{4.18}$$

d) Nhận xét về phương pháp

Các bảng 4.4 và 4.5 mô tả các nhận xét và đánh giá về kỹ thuật giấu tin trên miền hệ số.

Bảng 4.4. Bảng nhận xét về kỹ thuật sửa đổi hệ số DC

Ưu điểm	Nhược điểm
• Phương pháp này đơn giản và dễ hiểu, vì chỉ cần sửa đổi hệ số DC của khối 8x8. • Nó được sử dụng trong các định dạng hình ảnh phổ biến, chẳng hạn như JPEG, MPEG. • Giấu tin bằng phương pháp sửa đổi hệ số DC có độ bền cao, vì hệ số DC thường có giá trị lớn và được bảo vệ tốt hơn so với các hệ số AC.	• Phương pháp này có thể bị phát hiện bởi các kỹ thuật phân tích tần số. • Sửa đổi hệ số DC có thể ảnh hưởng đến chất lượng hình ảnh ban đầu, vì nó là một hệ số quan trọng trong việc xác định cường độ ánh sáng của khối.

Bảng 4.5. Nhận xét về kỹ thuật sửa đổi hệ số DC và AC với hệ số cân bằng độ lệch

Ưu điểm	Nhược điểm
• Kỹ thuật này có khả năng chống lại các phép tấn công thống kê, bởi vì nó sử dụng các hệ số cân bằng để làm cho sự thay đổi của các hệ số giấu tin ít dễ phát hiện hơn. • Kỹ thuật này cho phép giấu tin ở nhiều vị trí khác nhau trong khối hệ số, từ đó giúp tăng độ bảo mật và độ tin cậy của hệ thống.	• Kỹ thuật này có thể gây ra nhiễu trên khối hệ số và ảnh hưởng đến chất lượng của hình ảnh hoặc video. • Yêu cầu tính toán phức tạp và cồng kềnh.

4.4. Một số phương pháp khác

4.4.1. Phương pháp phát hiện thay đổi khung cảnh

a) Tổng quan chung

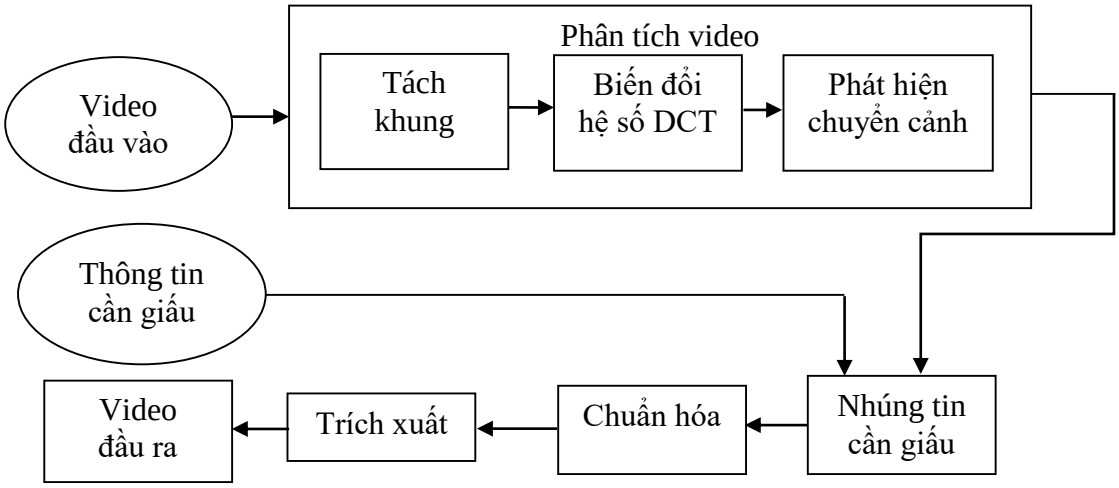
Phương pháp giấu tin trong video dựa trên kỹ thuật phát hiện chuyển cảnh (change scene detection) là phương pháp lợi dụng sự thay đổi các khung hình trong video để giấu thông tin. Về cơ bản thì mọi khung hình đều không giống nhau về kích thước. Bất cứ thay đổi nào giữa khung hiện tại và khung trước đó sẽ cho biết một sự thay đổi của cảnh. Trong chuyển cảnh sẽ bao gồm 2 loại [24]: Chuyển cảnh đột ngột (nhanh): Đây là những chuyển cảnh gây ra bởi việc chỉnh sửa của người làm video. Chuyển cảnh từ từ (chậm): Đây là những chuyển cảnh do việc quay của người làm video.

Phát hiện chuyển cảnh là kỹ thuật được sử dụng để phát hiện sự thay đổi trong một chuỗi video. Kỹ thuật phát hiện chuyển cảnh được sử dụng để tìm kiếm các điểm khác biệt giữa các khung hình trong một video. Có nhiều kỹ thuật và phương pháp khác nhau để có thể phát hiện chuyển cảnh bao gồm: sự khác biệt về điểm ảnh; tổng của chênh lệch tuyệt đối; chênh lệch thống kê, hình khối trong hình ảnh; sự khác biệt trong biểu đồ; sự chênh lệch của

ma trận DCT. Tuy nhiên, do những ưu điểm vượt trội của mình mà phương pháp phát hiện chuyển cảnh dựa trên sự chênh lệch dựa của ma trận DCT đang được áp dụng rộng rãi và phổ biến nhất hiện nay. Do đó, giáo trình sẽ sử dụng phương pháp này để làm cơ sở cho giấu tin vào video.

b) Quy trình giấu tin

Hình 4.15 trình bày tổng quan về quy trình giấu tin dựa trên sự thay đổi khung cảnh.



Hình 4.15. Quy trình giấu tin trong video dựa trên kỹ thuật phát hiện chuyển cảnh

Từ hình 4.15 thấy được quá trình giấu tin dựa trên phát hiện chuyển cảnh trải qua 3 giai đoạn chính [24, 25]:

- Video series parsing (Phân tích chuỗi video): Ở giai đoạn này video đầu vào là vật chứa sẽ được phân tích thành các frames (khung) riêng biệt. Sau đó từ các frames sẽ thực hiện biến đổi DCT để thu được các hệ số cosin rời rạc. Tiếp theo, từ những hệ số đã biết của các khối trên những khung hình, sẽ tiến hành phát hiện chuyển cảnh.
- Giấu tin: Sau khi đã phát hiện ra các khung cảnh thay đổi, có thể thỏa thuận với đối tượng cần trao đổi như: sẽ giấu vào khung chuyển cảnh nào, từ những khung đó sẽ xét xem thứ tự để giấu tin như thế nào, ở đây có thể dùng LSB hoặc một số kỹ thuật khác để giấu.
- Chuẩn hóa: Bước chuẩn hóa này nhằm mục đích hạn chế dư thừa dữ liệu, loại bỏ những phần tử cấu trúc phức tạp, nhưng vẫn đảm bảo không làm mất dữ liệu, tiết kiệm không gian lưu trữ.

Cụ thể chi tiết các bước tiến hành trong 3 giai đoạn trên được thực hiện như sau:

- Phân tích chuỗi video: ở bước phân tích chuỗi video sẽ tiến hành 3 nhiệm vụ là tách khung hình và biến đổi DCT và phát hiện chuyển cảnh. Đối với bước tách khung hình video ban đầu sẽ được tách ra thành các khung hình và từ những khung hình đã tách ra đó sẽ được biến đổi sang các hệ số cosin rời rạc DCT. Đối với bước biến đổi DCT thì từ những khung hình đã được tách hệ thống sẽ tiến hành xử lý trên từng khung hình nhằm biến đổi các hệ số từ miền không gian sang miền tần số. Trong chương 2 của giáo trình đã trình bày chi tiết về

quy trình biến đổi DCT. Đối với quá trình phát hiện chuyển cảnh thì sau khi đã có hệ số DCT cho mỗi khung hình hệ thống sẽ tiến hành tính toán sự khác biệt giữa các cặp khung hình để phát hiện ra sự thay đổi chuyển cảnh giữa các cặp khung hình. Việc tính toán sự khác biệt giữa các cặp khung hình dựa trên công thức 4.19:

$$D(f_k, f_{k+1}) = \sum u \sum v \left[C_k(u,v) - C_{k+1}(u,v)\right] \quad (4.19)$$

Trong đó:

- $D(f_k, f_{k+1})$ là giá trị điểm chuyển cảnh hay còn gọi giá trị chênh lệch khung của f_k và f_{k+1}
- f_k và f_{k+1} đại diện cho 2 khung hình liên tục
- f_k (u, v) là giá trị điểm ảnh tại vị trí (u, v).
- Các DC của các khung liên tiếp được biểu diễn bởi $C_k(u,v)$ và $C_{k+1}(u,v)$.

Dựa trên công thức trên. Giả sử 1 video có 100 khung hình, để phát hiện chuyển cảnh, sẽ lấy hiệu hệ số DCT của từng cặp giá trị điểm ảnh tương ứng mỗi khung hình f_k, f_{k+1} sau khi tính hiệu sẽ lấy tổng của chúng để tìm ra hệ số giá trị chênh lệch khung. Nếu video có 100 khung hình tức sẽ phải tính hiệu của 99 cặp khung hình để tìm ra được sự khác biệt giữa chúng. Thuật toán phát hiện chuyển cảnh có khả năng phát hiện ngay cả những thay đổi nhỏ nhất trong một cảnh. Khi đó, giá trị điểm chuyển cảnh sẽ đặt làm 1. Còn nếu không có sự thay đổi nào được phát hiện thì điểm chuyển cảnh sẽ đặt về 0. Và nếu điểm chuyển cảnh lớn hơn 0 thì thủy vân sẽ nhúng vào đấy.

- Giấu tin: Khi tìm được $D(f_k, f_{k+1}) > 0$ hoặc là 1 ngưỡng mà người nhúng và người kiểm, người giấu tin lấy ảnh f_{k+1} để bắt đầu việc giấu tin. Trong quá trình giấu, các bit tin giấu sẽ nhúng vào trong hệ số DCT của khối 8x8. Quá trình nhúng có thể được thực hiện bằng việc thay thế LSB hoặc phương pháp nào đó trên các hệ số DCT với các bit tin giấu.
- Chuẩn hóa: Chuẩn hóa là việc kết hợp kết quả của quá trình phân tích sóng ngắn video gốc và dữ liệu đã được giấu vào một thể duy nhất. Video gốc và tin giấu được chuẩn hóa trong khu vực DWT để cho các giá trị điểm ảnh của video (trong dạng số nguyên) từ 0-255, chỉ còn nằm trong khoảng 0 đến 1 của giá trị điểm ảnh chuẩn hóa. Mục đích của việc này là đảm bảo các giá trị điểm ảnh không vượt quá giá trị lớn nhất của các hệ số tương ứng trong quá trình kết hợp. Hơn nữa, sự thay đổi diễn ra trong video khi thông tin được giấu sẽ được giảm bớt khiến cho chất lượng video được tăng lên. Sau khi chuẩn hóa cả khung hình ảnh video gốc khung hình chứa tin mật, 2 hệ số DWT của chúng sẽ được kết hợp lại và tạo ra khung ảnh có giấu tin theo công thức 4.20:

$$S(p,q) = \alpha\, C(p,q) + \beta R(p,q) \quad (4.20)$$

Trong đó:

- $C(p,q)$ là hệ số DWT của ảnh trong video gốc.
- p,q chỉ các cột và hàng của điểm ảnh trong ảnh video gốc;
- S là hệ số DWT đã được chỉnh sửa của ảnh giấu tin;

- $R(p,q)$ là hệ số DWT của thủy vân;
- α, β là 2 yếu tố nhằm cải thiện độ bí mật của tin giấu và $\alpha + \beta = 1$. Hai yếu tố này được lựa chọn sao cho thủy vân là không thể phân biệt được trong video đã được nhúng

c) Quy trình tách tin

Quá trình tách tin nhằm mục đích khôi phục lại thông tin mật đã giấu là quá trình ngược của việc giấu tin. Đầu tiên người giấu tin và tách tin phải thỏa thuận chọn lựa các khung cảnh cùng với ngưỡng phát hiện chuyển cảnh. Cụ thể, mỗi khung cảnh sẽ được phân tích để thu được các hệ số DC. Hệ số DC này được sử dụng cho nhiệm vụ phát hiện các chuyển cảnh. Cuối cùng, từ hệ số phát hiện, các bit thông tin giấu được tách ra. Quá trình tách khôi phục tin nhắn được giấu HM_k bằng công thức 4.21:

$$HM_k(p,q) = (S_k(p,q) - C_k(p,q))/\delta_k \quad (4.21)$$

Trong đó:

- $S_{k(p,q)}$ là khung video giấu tin;
- $C_{k(p,q)}$ là video gốc;
- k là số khung;
- δk là yếu tố để điều chỉnh tính bền vững của video giấu mà đã sử dụng để đổi lại tính vô hình, sự bền vững và tính bí mật. Nếu như điểm chuyển cảnh lớn hơn 0 và bất cứ chuyển cảnh nào diễn ra trong các khung cảnh video được giấu thì thông tin được giấu sẽ được tách ra.

d) Nhận xét về phương pháp

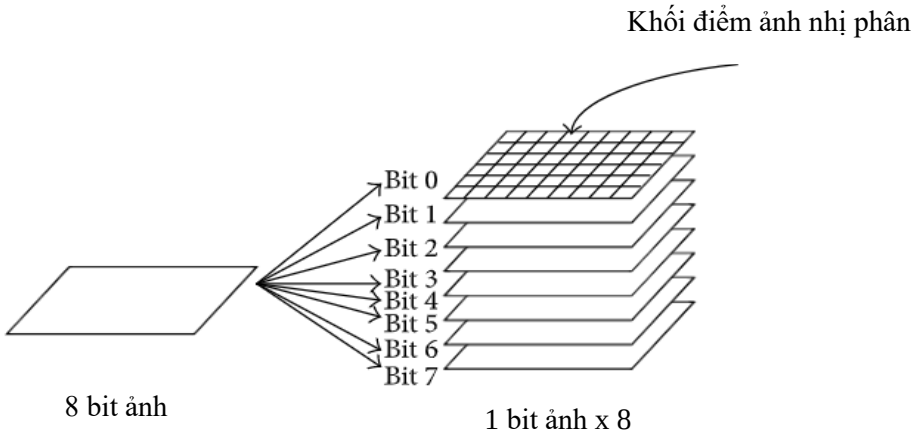
Về mặt lý thuyết có thể thấy rằng phương pháp giấu tin vào điểm chuyển cảnh trong video được cho là an toàn hơn so với giấu tin vào các khung hình bình thường vì các điểm chuyển cảnh có thể che giấu sự thay đổi do giấu tin gây ra. Ngoài ra, các điểm chuyển cảnh thường là những khu vực có nhiều chi tiết và màu sắc đa dạng, do đó, những thay đổi nhỏ của điểm ảnh tại các điểm này có thể bị che giấu bởi sự đa dạng của điểm ảnh và màu sắc trong khung hình. Bên cạnh đó, giấu tin vào các điểm chuyển cảnh trong video cũng giúp tăng tính bí mật của thông tin cần giấu, vì thường chỉ người nhận mới biết chính xác các ngưỡng chuyển cảnh để tìm thông tin giấu trong video. Điều này làm cho việc tìm kiếm và phát hiện các thông tin giấu trở nên khó khăn hơn. Đồng thời với hướng tiếp cận tìm kiếm các thay đổi trong chuyển cảnh, phương pháp này cho phép giấu tin với một lượng lớn dữ liệu bởi vì video thường có số khung hình rất lớn và có nhiều điểm chuyển cảnh. Tuy nhiên, xét về khía cạnh ứng dụng thực tế thì phương pháp giấu tin dựa trên phát hiện chuyển cảnh chủ yếu được áp dụng trong việc bảo vệ tin bí mật. Do đó, trong thực tế nếu chỉ sử dụng điểm chuyển cảnh một cách đơn thuần để giấu tin, thì thông tin cần giấu cũng không được quá lớn vì phương pháp này có thể làm ảnh hưởng đến chất lượng video. Một trong những nguyên nhân khác dẫn đến tình trạng này là phương pháp này thường chỉ sử dụng các đặc trưng thô

của video để phát hiện chuyển cảnh, điều này khiến cho phương pháp này có thể bị ảnh hưởng bởi độ phân giải thấp của video. Ngoài ra, phương pháp này không chống lại được một số kỹ thuật tấn công lên video như nén, xoay hoặc cắt....Để khắc phục các nhược điểm của kỹ thuật này, cần tập trung vào các phương pháp phát hiện chuyển cảnh mới. Theo đó, trong tài liệu [30] cũng đã liệt kê một số hướng tiếp cận khác cho phát hiện chuyển cảnh nhằm tím kiếm được các điểm chuyển cảnh mới và phù hợp hơn.

4.4.2. Phương pháp mặt phẳng bit

a) Giới thiệu

Phân đoạn độ phức tạp của các mặt phẳng bit (Bit-Plane Complexity Segmentation - BPCS) là một kỹ thuật giấu tin được phát minh bởi Eiji Kawaguchi và Richard O. Eason vào năm 1997. Đây là một kỹ thuật giấu tin sử dụng khung hình làm vật chứa tin. Đặc trưng của kỹ thuật này là khung hình ảnh được chia thành các mặt phẳng bit dựa trên giá trị độ sâu của hình ảnh. Mặt phẳng bit được định nghĩa là độ sâu màu của điểm ảnh. Ví dụ một khung hình (*n* x *n* điểm ảnh) với độ sâu màu 8 bit sẽ có 8 mặt phẳng. Tương tự với độ sâu màu là 24 và 32 thì sẽ có 24 mặt phẳng và 32 mặt phẳng. Hình 4.16 thể hiện ví dụ hình ảnh có độ sâu điểm ảnh là 8 bit được chia thành 8 mặt phẳng bit khác nhau.



Hình 4.16. Biểu diễn 1 điểm ảnh bit thành 8 mặt phẳng bit

Từ hình 4.16 có thể thấy, với các giá trị nhị phân và một phần của khung hình sẽ tạo được các mặt phẳng bit. Mỗi mặt phẳng bit là cấu trúc dữ liệu được làm từ tất cả các bit quan trọng nhất định từ mỗi chữ số nhị phân, với vị trí không gian được giữ nguyên. Ví dụ với khung hình 8x8 điểm ảnh với độ sâu màu 8 bit. Trong mặt phẳng bit sẽ biểu diễn như sau: Màu đen biểu diễn bit 0 và màu trắng biểu diễn bit 1. Điểm ảnh đầu tiên biểu diễn dưới dạng 01001110:

- Mặt phẳng bit thứ nhất tại (0,0) là ô màu đen (giá trị 0).
- Mặt phẳng bit thứ hai tại (0,0) là ô màu trắng (giá trị 1).

- ……
- Mặt phẳng bit thứ 8 tại (0,0) là ô màu đen (giá trị 0).

Mỗi mặt phẳng bit nếu là nhiễu có thể giấu được 1 bit thông điệp cần gửi đi. Theo phương pháp giấu tin dựa trên mặt phẳng bit thì thông tin sẽ được giấu vào các mặt phẳng bit mà có độ nhiễu cao. Để xác định được mặt phẳng bit có khối nhiễu cao hay thấp, có thể áp dụng phương pháp để tính ra độ phức tạp của mặt phẳng bit. Quy trình tính toán như sau:

- Độ phức tạp của mặt phẳng bit: Là sự chuyển tiếp từ bit 1 thành bit 0 và từ bit 0 thành bit 1 bao gồm cả chiều ngang và chiều dọc, không liên quan đến số lượng các giá trị 0 và 1.

- Ngưỡng phức tạp (α): là ranh giới phân biệt độ phức tạp cao và độ phức tạp thấp. Trong một số trường hợp, ngưỡng phức tạp được áp dụng để xác định vị trí các mặt phẳng bit để giấu thông tin. Trong thực tế, các chuyên gia đã thử nghiệm trên khối có kích thước khác nhau và thấy được việc sử dụng khối 8x8 là phù hợp nhất cho phương pháp giấu tin. Theo đó, với khối 8x8 thì các thông số về α được phát hiện là giá trị trung bình khoảng 0,5, những khối được xem là nhiều thông tin thì có α trong khoảng từ 0 – 0,5 và chỉ chiếm $6.67\times10^{-14}\%$. Từ những giá trị đó thông thường người ta sẽ chọn ngưỡng phức tạp là α_0 = 0.3 cho khối 8x8.

- Khối nhiều thông tin: là vùng có độ phức tạp thấp hơn ngưỡng phức tạp. Nếu thay đổi thông tin ở đây sẽ xảy ra sự thay đổi hình dạng của khung hình. Đây là vùng có nhiều thông tin quan trọng của hình ảnh, dẫn đến sự thay đổi lớn nếu thay đổi thông tin ở mặt phẳng bit này.

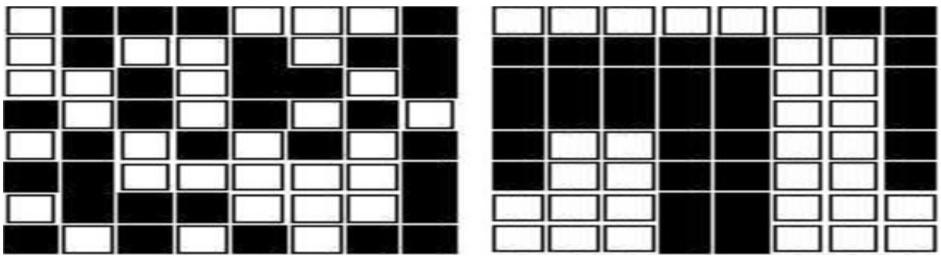
- Khối nhiễu: là vùng có độ phức tạp cao hơn ngưỡng phức tạp. Đây là vùng để giấu thông điệp vì đây là vùng ít thông tin quan trọng của hình ảnh. Do đó hệ thống thị giác của con người khó phát hiện được sự thay đổi. Nếu thay đổi không làm thay đổi quá nhiều đến chất lượng của hình ảnh. Trong thực tế phải chọn các mặt phẳng bit được gọi là nhiễu để giấu thông điệp vào đó. Thực tế cho thấy, bước quan trọng nhất trong BPCS là xác định được các khối nhiễu trong mặt phẳng bit một cách chính xác. Hiện nay, chưa có một định nghĩa chính xác như thế nào là nhiễu cũng như cách để xác định độ nhiễu một cách chính xác tuyệt đối. Một trong những cách thường dùng để xác định khối nhiễu đó là Black-White border. Đây là một cách tiếp cận cổ điển và đơn giản đối với vấn đề này. Trong Black-white border độ nhiễu được xác định bằng chiều dài của các đường biên của các vùng đen trắng trong khối theo chiều ngang và chiều dọc. Ví dụ với một ô đen với 4 ô xung quang là trắng thì đường biên là 4. Với một khối có đường biên càng dài thì độ phức tạp càng cao. Dựa vào định nghĩa trên sẽ có công thức xác định độ phức tạp của một khối có kích thước *2n x 2n* nhưu sau (xem công thức 4.22):

$$\alpha = \frac{k}{2\times2n\times(2n-1)} \tag{4.22}$$

Trong đó

- α là độ phức tạp của khối

- k là số đường viền tiếp xúc giữa 2 vùng
- $2 \times 2n \times (2n-1)$là số đường viền tiếp xúc nhiều nhất có thể với khối đó chính là số đường viền trong ô bàn cờ.

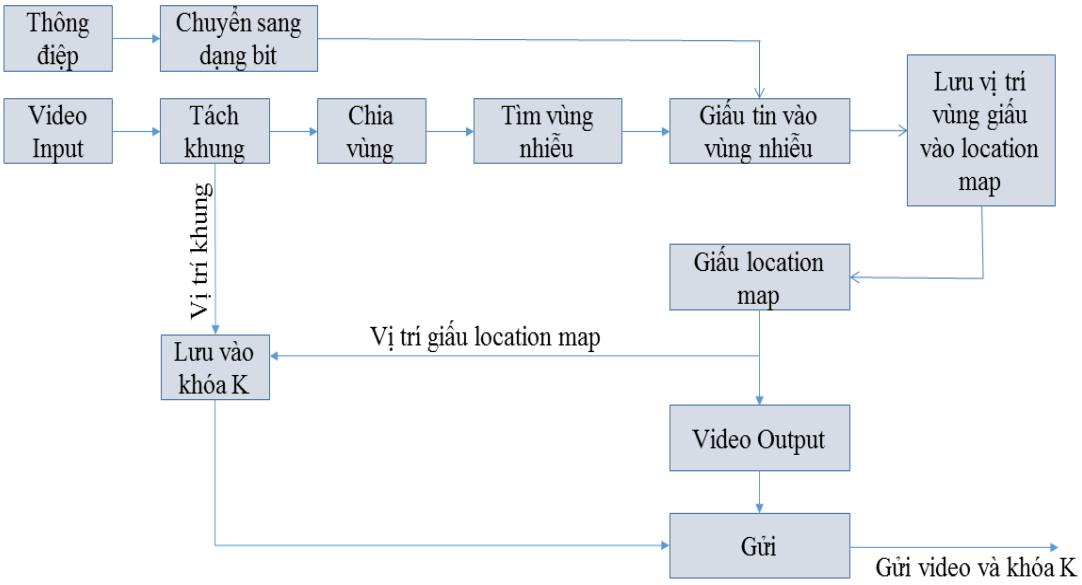


a) Vùng nhiễu b) Vùng nhiều thông tin

Hình 4.17. Phân loại vùng nhiễu và vùng nhiều thông tin

Dựa trên công thức ở trên, xem ví dụ về vùng nhiều và vùng nhiều thông tin được giới thiệu như hình 4.17. Trong đó màu trắng là giá trị 1 và màu đen là giá trị 0. Từ quy tắc tính như trên có thể thấy: Đối với hình 4.3(a) được coi là vùng nhiễu vì độ phức tạp của mặt phẳng bit là 69. Đối với hình 4.3(b) được coi là vùng nhiều thông tin vì độ phức tạp của mặt phẳng bit là 29. Như vậy thông tin sẽ được nhúng vào hình 4.3(a).

b) Quy trình giấu tin



Hình 4.18. Quy trình giấu tin trong video vào mặt phẳng bit

Từ sơ đồ quy trình giấu tin trong video như hình 4.18 thấy được các bước chính của kỹ thuật giấu tin vào mặt phẳng bit như sau [24, 27]:

- Bước 1. Tiền xử lý dữ liệu: với 2 thông tin đầu vào là video input và thông tin mật người giấu tin cần thực hiện:

- Đối với thông tin mật: chuyển thông tin mật thành dạng nhị phân.
- Đối với video input: tiến hành tách video thành các khung hình. Chọn một khung ảnh bất kì để chuẩn bị giấu thông tin mật. Việc chọn vị trí khung sẽ được lưu vào khóa *K*. Vị trí này sau này sẽ hỗ trợ cho người tách tin tìm thấy khung hình để tách tin. Sau khi chọn được khung hình sẽ tiến hành chia vùng để tạo thành các mặt phẳng bit. Mỗi điểm ảnh có độ sâu màu là 8, 24, 32 bit thì sẽ có 8, 24, 32 mặt phẳng bit tương ứng. Tiếp theo là đến giai đoạn tìm vùng nhiễu. Theo đó, tại khung hình vừa lựa chọn, sau khi đã xác định độ sâu của ảnh, người giấu tin sẽ tính toán độ phức tạp của mặt phẳng để tìm xem đâu là vùng nhiễu đâu là vùng nhiều thông tin. Quy trình tính toán để xác định vùng nhiều và vùng nhiều thông tin đã được trình bày ở bước trên.
- Bước 2. Giấu tin mật: Thông điệp được chuyển dạng nhị phân rồi giấu vào vùng nhiễu đã được tìm ra ở trên. Phương pháp giấu thông tin mật vào vùng nhiễu có thể lựa chọn sử dụng phương pháp thay thế LSB. Tiếp đến người giấu tin cần lưu vị trí các khối nhiễu vào location map để làm cơ sở cho người tách tin tìm ra các vị trí tin giấu. Người giấu tin cũng có thể nhúng cả location map cùng các khối bí mật và chỉ lưu vị trí của khối này hoặc lưu trữ riêng cả location map này vào khóa *K*. Cuối cùng người giấu tin sẽ chuyển video đã giấu tin và khoá *K* cho bên nhận.

c) Quy trình tách tin

Sau khi bên nhận nhận được khóa *K* và video chứa tin sẽ bắt đầu phân tích để thu thập được thông tin giấu. Các bước tiến hành trong quy trình tách tin như sau:

- Bước 1: Thực hiện tách video thành các khung. Thông thường video có tốc độ là 60fps (tốc độ chuẩn để mắt người không cảm nhận được khoảng chuyển đổi giữa các khung hình), tức là 60 khung hình/s, do đó nếu video dài 1 phút ta có thể tách được 60x60 = 3600 khung hình.
- Bước 2: Tách khóa *K* để thu được:
- Vị trí Location map: Được lưu dưới dạng [Vị trí khung chứa, Mặt phẳng bit chứa, Tọa độ khối bí mật chứa nó]. Dựa vào vị trí location map, xác định khung chứa Location map.
- Vị trí khung chứa tin.
- Bước 3: Cắt khung đó thành các mặt phẳng bit, xác định các mặt phẳng chứa, xác định các khối chứa tin và tách, thu được Location map:
- Location map được lưu dưới dạng [Vị trí khối bí mật 1, Vị trí khối bí mật 2, ...]
- Vị trí khối bí mật thứ i có dạng [Mặt phẳng bit, Tọa độ khối]
- Bước 4: Tìm khung chứa tin dựa vào vị trí khung chứa tin và các khung đã tách từ video sau đó tách khung chứa tin thành các mặt phẳng bit. Cuối cùng thực hiện tách các khối bí mật trong các mặt phẳng bit sẽ thu được thông tin giấu.

d) Nhận xét về phương pháp

Từ quy trình giấu tin và tách tin được mô tả ở trên, có thể nhận thấy rằng phương pháp BPCS tương đối đơn giản và dễ hiểu, dễ cài đặt. Ngoài ra, do BPCS là giấu tin trên các vùng nhiễu thay vì giấu trên tất cả các vùng, vì thế phương pháp này khiến việc phát hiện tin được giấu khó khăn hơn, giúp cho việc ứng dụng vào trong đời sống hiệu quả hơn. Tuy nhiên, phương pháp này rất kém hiệu quả với ảnh đã qua chỉnh sửa bởi vì các kỹ thuật hình học trong xử lý ảnh như: làm mịn, co giãn ảnh, khử nhiễu, … làm ảnh hưởng đến số lượng các vùng nhiễu, khiến việc lựa chọn vùng giấu tin trở nên khó khăn và tạo ra các dấu vết rõ ràng, khiến tin giấu dễ bị phát hiện. Để khắc phục nhược điểm của phương pháp BPCS, trong các nghiên cứu [26, 31], đã trình bày một số hướng tiếp cận tập trung mới tập trung theo 2 hướng chính là kỹ thuật tính toán độ nhiễu mới và phương pháp giấu tin tối ưu. Cụ thể, Đỗ Xuân Chợ [26] và các cộng sự đã trình bày một số hướng tiếp cận mới nhằm nâng cao khả năng giấu tin của phương pháp PBCS. Trong phần thực nghiệm, nhóm tác giả tập trung vào việc cải tiến công thức tính toán độ nhiễu của các mặt phẳng bit. Chi tiết các thuật toán và kỹ thuật này đã được mô tả trong [26, 31].

4.5. Tổng kết chương 4

Trong chương 4, giáo trình đã trình bày và phân tích một số nội dung sau:

- Giới thiệu tổng quan về nguyên tắc, đặc điểm và phân loại kỹ thuật giấu tin trong video.

- Trình bày và phân tích đặc điểm, nguyên tắc hoạt động của một số thuật toán giấu tin trong video dựa 2 hệ số chính là, DC, kết hợp AC, DC và cân bằng đồ lệch.

- Mô tả quy trình giấu tin, tách tin và đánh giá một số kỹ thuật giấu tin trong video dựa trên miền nén của video. Nhìn chung, phương pháp này có ưu điểm là giấu được nhiều thông tin và không tác động nhiều lên vật chứa. Tuy nhiên, nhược điểm của chúng là quy trình giấu tin tương đối phức tạp. Đặc biệt sau khi giấu tin xong, người giấu tin cần phải tiến hành mã hóa lại video cho đúng chuẩn. Quá trình này đòi hỏi người giấu tin phải thực hiện đúng cách nếu không dung lượng video sẽ bị tăng đột biến và dễ làm mất mát thông tin giấu.

- Liệt kê và phân tích một số kỹ thuật giấu tin trong video khác dựa trên BPCS và phát hiện chuyển cảnh. Các phương pháp này được tiến hành tương đối thô sơ và đơn giản. Độ an toàn của thuật toán phụ thuộc vào việc giữ bí mật về vị trí giấu cũng và ngưỡng.

4.6. Câu hỏi ôn tập

Câu 1. Hãy trình bày về khái niệm phương pháp giấu tin trong video ? Hãy nêu các yêu cầu đối với kỹ thuật giấu tin trong video ?

Câu 2. Hãy liệt kê các phương pháp phân loại giấu tin trong video ?

Câu 3. Hãy trình bày phương pháp giấu tin trong video sử dụng kỹ thuật phát hiện chuyển cảnh ? Hãy vẽ sơ đồ thể hiện quá trình giấu tin và tách tin trong video bằng kỹ thuật phát hiện chuyển cảnh ?

Câu 4. Hãy trình bày khái niệm về chuẩn MPEG? Hãy trình bày khái niệm về giấu tin trong miền hệ số của video theo chuẩn MPEG?

Câu 5. Hãy trình bày về quy trình giấu tin trong video sử dụng phương pháp mặt phẳng bit? Hãy vẽ sơ đồ minh họa quá trình giấu tin và tách tin sử dụng kỹ thuật mặt phẳng bit

Câu 6 . Phân tích ưu điểm và nhược điểm của kỹ thuật giấu tin trong video sử dụng phương pháp mặt phẳng bit ?

Câu 7. Hãy trình bày về quy trình giấu tin trong video sử dụng kỹ thuật thay đổi hệ số AC? Hãy vẽ sơ đồ minh họa quá trình giấu tin và tách tin bằng kỹ thuật thay đổ hệ số AC?

Câu 8. Trình bày và phân tích ưu điểm và nhược điểm của kỹ thuật giấu tin trong video sử dụng kỹ thuật thay đổi hệ số AC ?

Câu 9. Hãy trình bày về phương pháp giấu tin trong videosử dụng kỹ thuật thay đổi hệ số DC? Hãy vẽ sơ đồ minh họa quá trình giấu tin và tách tin bằng kỹ thuật thay đổ hệ số DC?

Câu 10. Trình bày và phân tích ưu điểm và nhược điểm của kỹ thuật giấu tin trong video sử dụng kỹ thuật thay đổi hệ số DC ?

Câu 11. Hãy trình bày về phương pháp giấu tin trong video sử dụng kỹ thuật thay đổi hệ số DC, AC và cân bằng độ lệch?

Câu 12. Trình bày và phân tích ưu điểm và nhược điểm của kỹ thuật giấu tin trong video sử dụng kỹ thuật thay đổi hệ số DC, AC và cân bằng độ lệch?

Câu 13. Hãy trình bày về phương pháp giấu tin trong video dựa trên sự khác biệt năng lượng? Hãy vẽ sơ đồ minh họa quá trình giấu tin và tách tin của kỹ thuật giấu tin dựa trên sự khác biệt năng lượng.

Câu 14. Trình bày và phân tích ưu điểm và nhược điểm của kỹ thuật giấu tin trong video dựa trên sự khác biệt năng lượng?

Câu 15. Cho tin cần giấu: "*M* " và một file video (tự chọn). Bằng ngôn ngữ lập trình hãy thực hiện các yêu cầu sau:

a) Trích xuất một khung hình trong video ở trên.
b) Xuất ra màn hình 8 mặt phẳng bít.
c) Tính độ nhiễu của các mặt phẳng bit.
d) Chọn ngưỡng phức tạp là 0,3 hãy thực hiện giấu tin vào mặt phẳng bit đã được lưa chọn.

Câu 16. Cho tin cần giấu: "*M* " và một file video (tự chọn). Bằng ngôn ngữ lập trình hãy thực hiện các yêu cầu sau:

a) Thực hiện tính toán sự khác biệt giữa 3 cặp khung hình đầu tiên.
b) Thực hiện giấu tin vào khung hình có sự khác biệt lớn nhất theo phương pháp phát hiện chuyển cảnh.

Câu 17. Cho tin cần giấu: "*M* " và một file video (tự chọn). Bằng ngôn ngữ lập trình hãy thực hiện các yêu cầu sau:

a) Hãy thực hiện giấu tin vào video theo miền hệ số AC, DC; kết hợp AC với DC và cân bằng độ lệch.
b) Hãy so sánh chất lượng của khung hình đã giấu tin theo 3 phương pháp AC, DC; kết hợp AC với DC và cân bằng độ lệch dựa trên ma trận điểm ảnh của khung hình đã giấu.

TÀI LIỆU THAM KHẢO

[1] Konakhovich Georgiy Filimonovich; Puzyrenko Alexander Yurievich. Computer Steganography. Theory and practice. "MK-Press", 2019; 288p.

[2] Fabien A. Petitcolas, Stefan Katzenbeisser. Information Hiding Techniques for Steganography and Digital Watermarking. Boston, London: Artech House, 2000. 220 pages.

[3] Nguyễn Xuân Huy, Trần Quốc Dũng, Giáo trình giấu tin và thủy vân ảnh, Trung tâm thông tin tư liệu, TTKHTN – CN 2003.

[4] Birgit Pfitzmann, Matthias Schunter, "Asymmetric Fingerprinting". International Conference on the Theory and Applications of Cryptographic Techniques. EUROCRYPT 1996. pp 84-95.

[5] Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton Kalker, Digital Watermarking and Steganography. Second Edition. Morgan Kaufmann Publishers is an imprint of Elsevier. 2008, 593 pages.

[6] Microsoft Windows Bitmap File Format Summary. https://www.fileformat.info/format/bmp/egff.htm. [truy cập 5/2023].

[7] Mark Adler et al. Portable Network Graphics (PNG) Specification (Third Edition). 2022, [Available]: https://www.w3.org/TR/png-3/. [truy cập 5/2023].

[8] JPEG File Interchange Format Version 1.02 [Available]: https://www.w3.org/Graphics/JPEG/jfif3.pdf. [truy cập 5/2023].

[9] ITU, Information technology – digital compression and coding ofcontinuous-tone still images – requirements and guidelines (ISO/IEC 10918-1: 1993). [Available]: https://www.w3.org/Graphics/JPEG/itu-t81.pdf. [truy cập 5/2023].

[10] Shih, Frank Y. Digital Watermarking and Steganography: Fundamentals and Techniques (Second Edition). Taylor & Francis, CRC Press, 2017. 270 pages

[11] Unik Lokhande. A. K. Gulve Steganography using Cryptography and Pseudo Random Numbers. International Journal of Computer Applications International Journal of Computer Applications. 96 (19), 2014. pp.40-45. DOI:10.5120/16905-6977.

[12] Andrey Sidorenko and Berry Schoenmakers. Concrete Security of the Blum-Blum-Shub Pseudorandom Generator. Cryptography and Coding: 10th IMA International Conference, Lecture Notes in Computer Science. 2005. pp. 355-375.

[13] Po-Yueh Chen and Hung-Ju Lin, "A DWT Based Approach for Image Steganography", International Journal of Applied Science and Engineering. 4, 3, 2006, pp. 275-290,

[14] Chun-Shien Lu, Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property, Idea Group Publishing, 2005, 350 pages.

[15] Vijay Kumar, Dinesh Kumar. A modified DWT-based image steganography technique. Multimedia Tools and Applications. Volume 77, 2018, pp13279–13308.
[16] Pramanik, S. An adaptive image steganography approach depending on integer wavelet transform and genetic algorithm. Multimed Tools Appl (2023). https://doi.org/10.1007/s11042-023-14505-y
[17] Pradeep Kumar Singh, R.K.Aggrawal: Enhancement of LSB based Steganography for Hiding Image in Audio. International Journal on Computer Science and Engineering Vol 2, (5), 2010, pp. 1652-1658.
[18] Brian Moore. An introduction to the Psychology of Hearing, Sixth Edition, BRILL. 2013, 458 pages
[19] Đỗ Quốc Trinh, Vũ Thanh Hải: Kĩ thuật trải phổ và ứng dụng. Học viện kĩ thuật quân sự. 2006. 153 trang.
[20] L. Boney, A. H. Tewfik and K. N. Hamdy, "Digital watermarks for audio signals," Proceedings of the Third IEEE International Conference on Multimedia Computing and Systems, Hiroshima, Japan, 1996, pp. 473-480, doi: 10.1109/MMCS.1996.535015.
[21] I.J.COX, " Spread Spectrue Watermark for Embedled Signaling" United states Patent 5,848,155, December 1988.
[22] I. J. Cox, M. L. Miller and A. L. McKellips, "Watermarking as communications with side information," in Proceedings of the IEEE, vol. 87, no. 7, pp. 1127-1141, July 1999, doi: 10.1109/5.771068.
[23] H. S. Malvar and D. A. F. Florencio, "Improved spread spectrum: a new modulation technique for robust watermarking," in IEEE Transactions on Signal Processing, vol. 51, no. 4, pp. 898-905, April 2003, doi: 10.1109/TSP.2003.809385..
[24] Gerrit Cornelis. Real-time Watermarking Techniques for Compressed Video Data. Veenendaal ISBN 90-9013190-6. 2000. 158 pages.
[25] What Are the Different Types of Video Formats. [Available]: https://mailchimp.com/resources/video-formats/. [truy cập 5/2023].
[26] Cho Do Xuan, "A Proposal to Improve the Bit Plane Steganography based on the Complexity Calculation Technique" International Journal of Advanced Computer Science and Applications(IJACSA), 12 (6), 2021. http://dx.doi.org/10.14569/IJACSA.2021.0120659
[27] Djebbar. F, Ayad. B. Audio Steganograpgy by Phase Modification. International Conference on Emerging Security Information, Systems and Technologies, Lisbon, Portugal, 2014, pp. 31-35.
[28] Kadir Tekeli, Rifat Asliyan, " A comparison of echo hiding methods," The Eurasia Proceedings of Science, Technology, Engineering & Mathematics. Volume 1, 2017, pp.397-403.

[29] Hyoung Joong Kim, Yong Hee Choi. A novel echo-hiding scheme with backward and forward kernels. in IEEE Transactions on Circuits and Systems for Video Technology, vol. 13, no. 8, pp. 885-889, Aug. 2003, doi: 10.1109/TCSVT.2003.815950.

[30] Dolley Shukla, Chandra Shekhar Mithlesh, Manisha Sharma. A Survey on Different Video Scene Change Detection Techniques. International Journal of Science and Research International Journal of Science and Research (IJSR). 2013, pp. 2319-7064.

[31] S. Sun. A New Information Hiding Method Based on Improved BPCS Steganography. Advances in Multimedia. 2015, Article ID 698492 https://doi.org/10.1155/2015/698492.

[32] Đỗ Xuân Chợ, Bài giảng các kỹ thuật giấu tin, Học viện công nghệ bưu chính viễn thông, 2018, 150 trang.

[33] Audio-steganography-algorithms. GitHub - ktekeli/audio-steganography-algorithms: A Library of Audio Steganography & Watermarking Algorithms. [truy cập 5/2023].

[34] Nguyễn Bình, Ngô Đức Thiện. *Cơ sở mật mã học*. Học Viện Công Nghệ Bưu Chính Viễn Thông, 2013. 237 trang.

[35] Video-steganography. https://github.com/topics/video-steganography. [truy cập 5/2023].

[36] Image-steganography-tool. https://github.com/topics/image-steganography-tool. [truy cập 5/2023].