

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG



ĐỖ XUÂN CHỢ

BÀI GIẢNG

CÁC KỸ THUẬT GIẤU TIN

Hà Nội, tháng 12 năm 2018

MỞ ĐẦU

Kỹ thuật giấu tin là 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 và 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. Việc triển khai các kỹ thuật giấu tin trong thực tế đã và đang mang lại hiệu quả rất lớn không chỉ trong lĩnh vực đảm bảo an toàn thông tin mà còn trong rất nhiều lĩnh vực khác. 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 và phát hiện giấu tin trong môi trường đa phương tiện, trong văn bản; một số ứng dụng của các kỹ thuật giấu tin đang được triển khai trong thực tế.

Bài giảng “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 nghiên cứu và học tập. Bài giảng 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....

Chương 2: Giấu tin trong ảnh. Chương 2 cung cấp các kiến thức về kỹ thuật giấu tin và tách tin trong ảnh tĩnh. Một số phương pháp giấu tin trong ảnh tĩnh hiện nay bao gồm: LSB, hoán vị giả ngẫu nhiên, kỹ thuật biến đổi DCT, DWT... Bên cạnh đó, trong chương 2 bài giảng còn cung cấp một số phương pháp phát hiện ảnh tĩnh có giấu tin.

Chương 3: Giấu tin trong âm thanh. Chương 3 trình bày một số kiến thức liên quan đến 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. Ngoài ra, chương 3 đề cập đến một số phương pháp, kỹ thuật phát hiện giấu tin trong âm thanh.

Chương 4: Giấu tin trong video. Chương này trình bày một số kiến thức liên quan đến kỹ thuật giấu tin và tách tin trong video. Bên cạnh đó, trong chương này bài giảng đề cập đến một số phương pháp phát hiện tin giấu trong video.

Chương 5: Giấu tin trong văn bản. Trong chương trình bày một số kiến thức liên quan đến kỹ thuật giấu tin trong văn bản 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. Ngoài ra, chương 5 đề cập đến một số phương pháp, kỹ thuật phát hiện giấu tin trong văn bản.

MỤC LỤC

DANH MỤC CÁC TỪ VIẾT TẮT	6
CHƯƠNG 1: TỔNG QUAN VỀ GIẤU TIN.....	10
1.1. Tổng quan về kỹ thuật giấu tin	10
<i>1.1.1. Một số thuật ngữ và khái niệm cơ bản</i>	<i>10</i>
<i>1.1.2. Một số yêu cầu đối với kỹ thuật giấu tin</i>	<i>11</i>
<i>1.1.3. Lịch sử phát triển</i>	<i>12</i>
<i>1.1.4. Vai trò và tầm quan trọng</i>	<i>13</i>
1.2. Phân loại các kỹ thuật giấu tin	15
<i>1.2.1. Phân loại theo vật chứa</i>	<i>15</i>
<i>1.2.2. Phân loại theo môi trường giấu tin</i>	<i>16</i>
<i>1.2.3. Phân loại theo cách thức tác động lên vật chứa tin</i>	<i>17</i>
<i>1.2.4. Phân loại theo mục đích sử dụng</i>	<i>17</i>
<i>1.2.5. Phân loại theo theo giao thức</i>	<i>20</i>
1.3. Một số ứng dụng của kỹ thuật giấu tin.....	21
<i>1.3.1. Lấy dấu vân tay (fingerprinting)</i>	<i>21</i>
<i>1.3.2. Xác thực nội dung (content authentication)</i>	<i>22</i>
<i>1.3.3. Kiểm soát sao chép (copy control)</i>	<i>23</i>
<i>1.3.4. Bảo vệ bản quyền tác giả (Copyright protection)</i>	<i>25</i>
<i>1.3.5. Một số ứng dụng khác</i>	<i>25</i>
1.4. Câu hỏi ôn tập.....	25
CHƯƠNG 2: GIẤU TIN TRONG ẢNH	27
2.1. Một số vấn đề trong giấu tin trong ảnh.....	27
<i>2.1.1. Khái niệm và yêu cầu của kỹ thuật giấu trong ảnh</i>	<i>27</i>
<i>2.1.2. Một số định dạng ảnh.....</i>	<i>27</i>
<i>2.1.3. Phân loại kỹ thuật giấu tin trong ảnh</i>	<i>30</i>
2.2. Phương pháp giấu tin trên miền không gian	31
<i>2.2.1. Phương pháp thay thế</i>	<i>31</i>
<i>2.2.2. Phương pháp hoán vị giả ngẫu nhiên</i>	<i>33</i>
2.3. Phương pháp giấu tin trên miền tần số	36
<i>2.3.1. Phương pháp biến đổi miền tần số DCT</i>	<i>36</i>
<i>2.3.2. Phương pháp biến đổi DWT</i>	<i>44</i>

2.4. Phương pháp phát hiện giấu tin trong ảnh.....	55
2.4. Câu hỏi ôn tập.....	56
CHƯƠNG 3: GIẤU TIN TRONG ÂM THANH.....	58
3.1. Giới thiệu về giấu tin trong âm thanh	58
3.1.1. Đặc điểm của kỹ thuật giấu tin trong âm thanh	58
3.1.2. Một số định dạng file âm thanh	59
3.1.3. Phân loại một số phương pháp giấu tin trong âm thanh	60
3.2. Phương pháp LSB	61
3.3. Phương pháp mã hóa pha.....	63
3.3.1. Khái niệm về phương pháp mã hóa pha	63
3.3.2. Quy trình giấu tin bằng phương pháp mã hóa pha	64
3.3.3. Đánh giá về phương pháp mã hóa pha	67
3.4. Một số phương pháp khác	67
3.4.1. Phương pháp tự đánh dấu	67
3.4.2. Phương pháp trải phổ	70
3.4.3. Phương pháp Echo	80
3.5. Phương pháp phát hiện giấu tin trong âm thanh.....	84
3.6. Câu hỏi ôn tập.....	85
CHƯƠNG 4: GIẤU TIN TRONG VIDEO	87
4.1. Giới thiệu về phương pháp giấu tin trong video	87
4.1.1. Đặc điểm của giấu tin trong video	87
4.1.2. Một số định dạng file video	87
4.1.3. Phân loại kỹ thuật giấu tin trong video	89
4.2. Phương pháp giấu tin trong video	90
4.2.1. Phương pháp phát hiện thay đổi khung cảnh	90
4.2.2. Phương pháp mặt phẳng bit	93
4.2.3. Phương pháp giấu trong miền video nén dựa trên sự khác biệt năng lượng ...	96
4.2.4. Phương pháp giấu trên miền nén của video chất lượng cao	100
4.2.5. Phương pháp giấu tin trong miền hệ số.....	105
4.3. Phương pháp phát hiện giấu tin trong video	109
4.4. Câu hỏi ôn tập.....	110
CHƯƠNG 5: GIẤU TIN TRONG VĂN BẢN	112
5.1. Đặc điểm của giấu tin trong văn bản.....	112
5.1.1. Giới thiệu chung	112

5.1.2. Một số định dạng văn bản điển hình	112
5.1.3. Phân loại phương pháp giấu tin trong văn bản	114
5.2. Phương pháp dựa trên định dạng văn bản	115
5.2.1. Phương pháp sử dụng khoảng trắng	115
5.2.2. Phương pháp dịch chuyển vị trí dòng	118
5.2.3. Phương pháp dịch chuyển vị trí từ	120
5.3. Phương pháp sinh ngẫu nhiên và thống kê.....	120
5.3.1. Phương pháp sử dụng văn phạm phi ngữ cảnh	120
5.3.2. Phương pháp dựa trên tính phản xạ đối xứng của ký tự	124
5.4. Phương pháp sử dụng tính chất ngôn ngữ.....	129
5.4.1. Phương pháp sử dụng cú pháp	129
5.4.2. Phương pháp sử dụng ngữ nghĩa	130
5.5. Phương pháp phát hiện giấu tin trong văn bản	131
5.6. Câu hỏi ôn tập.....	132
TÀI LIỆU THAM KHẢO.....	134

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

TT Bảng	Nội dung	Trang
Bảng 2.1	Cấu trúc tập tin Bitmap	29
Bảng 2.2	Các giá trị trong tiêu đề tập tin PNG	30
Bảng 2.3	Mô tả một số cờ thông dụng trong ảnh JPEG [9]	31
Bảng 3.1	Một số phần mềm hỗ trợ giấu tin trong âm thanh	61
Bảng 4.1	Phân loại và bảng Huffman cho thành phần DC	102
Bảng 4.2	Huffman các hệ số AC	103
Bảng 5.1	Phân nhóm dựa trên tính phản xạ đối xứng theo trục ngang	125
Bảng 5.2	Phân nhóm dựa trên tính phản xạ đối xứng theo trục dọc	126
Bảng 5.3	Phân nhóm dựa trên tính phản xạ đối xứng theo trục ngang và trục dọc	126
Bảng 5.4	Mã hóa các ký tự Tiếng Việt thành cặp bit	130

DANH MỤC CÁC HÌNH VẼ

Hình 1.1. Mô hình chung cho quá trình giấu và tách tin	10
Hình 1.2. Phân loại các kỹ thuật giấu tin	15
Hình 1.3. Phân loại các phương pháp thủy vân số.....	18
Hình 1.4. Ứng dụng giấu tin trong kiểm soát sao chép	24
Hình 2.1. Bit có trọng số thấp LSB.....	31
Hình 2.2. Sơ đồ nhúng và tách tin của phương pháp hoán vị giả ngẫu nhiên	34
Hình 2.3. Sơ đồ tổng quan về quá trình giấu tin trong ảnh sử dụng phương pháp biến đổi DCT	37
Hình 2.4. Thuật toán zigzac	43
Hình 2.5. Quy trình giấu tin trong ảnh sử dụng kỹ thuật biến đổi DWT.....	44
Hình 2.6. Quét theo chiều ngang	45
Hình 2.7. Quét theo chiều dọc	46
Hình 2.8. Hình ảnh gốc so với ảnh đã biến đổi DWT	46
Hình 2.9. Mô hình tách tin trong kỹ thuật DWT	55
Hình 3.1. Ví dụ về tín hiệu âm thanh và mẫu	59
Hình 3.2. Mô tả phương pháp thay thế bit trong thuật toán LSB	62
Hình 3.3. Giấu tin sử dụng 4 bit LSB	63
Hình 3.4. Kỹ thuật giấu tin trong âm thanh dựa vào 7 bit MSB và 4 bit LSB	63
Hình 3.5. Mô tả chia âm thanh gốc thành các segment bằng nhau.....	65
Hình 3.6. Minh họa khi mỗi đoạn được biến đổi bằng DFT	65
Hình 3.7. Tín hiệu được giấu trong pha của đoạn đầu tiên.....	66
Hình 3.8. Ma trận pha mới được tạo	66
Hình 3.9. Pha mới được tạo ra sau khi kết hợp cường độ của pha cũ	66
Hình 3.10. So sánh pha trước và sau khi giấu tin	67
Hình 3.11. Quy tắc giấu thông tin sử dụng phương pháp điều chỉnh tỉ lệ thời gian.....	68
Hình 3.12. Ý tưởng trải phổ truyền thống	72
Hình 3.13. Minh họa về trải phổ nhảy tần	73
Hình 3.14. Sơ đồ khối của hệ thống trải phổ FHSS.....	74
Hình 3.15. Biểu đồ tần số của tần nhanh với FSK.....	75

Hình 3.16. Minh họa trải phổ dây trực tiếp	77
Hình 3.17. Sơ đồ khối hệ thống trải phổ DSSS	77
Hình 3.18. Bộ điều chế BPSK	79
Hình 3.19. Các tham số chính trong phương pháp mã hóa tiếng vang.....	81
Hình 3.20. Sơ đồ tổng quát phương pháp mã hóa tiếng vang	82
Hình 3.21. Nhân 0 và nhân 1	82
Hình 3.22. Đầu vào và đầu ra bước 2	83
Hình 3.23. Ví dụ giấu bit 0 và bit 1	83
Hình 3.24. Kết quả tiếng vang sử dụng nhân 0 và nhân 1	84
Hình 3.25. Kết quả của hàm trộn	84
Hình 3.26. Phân loại các kỹ thuật phát hiện giấu tin trong âm thanh.....	85
Hình 4.1. Quy trình giấu tin trong video dựa trên kỹ thuật phát hiện chuyển cảnh	91
Hình 4.2. Biểu diễn 1 điểm ảnh bit thành 8 mặt phẳng bit	94
Hình 4.3. Phân loại vùng nhiễu và vùng nhiễu thông tin	95
Hình 4.4. Quy trình giấu tin trong video vào mặt phẳng bit.....	95
Hình 4.5. Sơ đồ tổng quát phương pháp giấu tin trong miền video nén dựa bằng DEW ...	97
Hình 4.6. Ví dụ về việc chia khối lc	98
Hình 4.7. Quá trình tính toán năng lượng trong vùng lc.....	98
Hình 4.8. Quy trình giấu tin trong nội dung video MPEG -2	100
Hình 4.9. Quy trình mã hóa entropy thành phần hệ số DC	101
Hình 4.10. Quy trình mã hóa entropy thành phần hệ số AC	102
Hình 4.11. Thay thế giá trị cho thông tin cần giấu trong QIM	105
Hình 4.12. Mô hình tổng quát kỹ thuật giấu tin trong miền hệ số.....	106
Hình 4.13. Quy trình giấu tin trong video bằng kỹ thuật sửa đổi hệ số DC	107
Hình 4.14. Quy trình giấu tin trong video bằng kỹ thuật sửa đổi hệ số DC và AC với hệ số cân bằng độ lệch	108
Hình 5.1. Một số vị trí khoảng trống có thể lựa chọn để giấu tin	115

CHƯƠNG 1: TỔNG QUAN VỀ GIẤU TIN

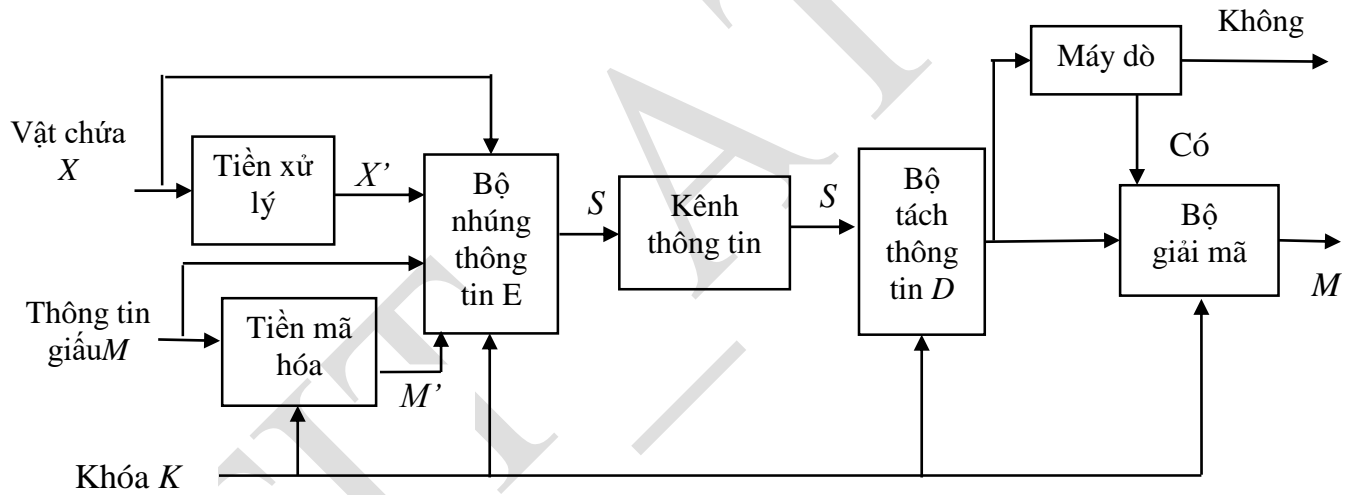
Chương này cung cấp các kiến thức cơ bản liên quan đến kỹ thuật giấu tin bao gồm: khái niệm, các thuật ngữ, phân loại, một số ứng dụng cơ bản.

1.1. Tổng quan về kỹ thuật giấu tin

1.1.1. Một số thuật ngữ và khái niệm cơ bản

a) Khái niệm về kỹ thuật giấu tin

Kỹ thuật giấu thông tin là lĩnh vực chuyên nghiên cứu về các phương pháp, kỹ thuật, thuật toán nhằm nhúng thông tin vào một đối tượng dữ liệu khác. Cũng giống như mật mã học, kỹ thuật giấu tin bao gồm nhiều phương pháp, thuật toán và kỹ thuật khác nhau. Mỗi phương pháp, thuật toán và kỹ thuật có những yêu cầu về đầu vào và đầu ra khác nhau. Tuy nhiên, một hệ thống giấu tin sẽ bao gồm các thành phần sau (xem hình 1.1) [1].



Hình 1.1. Mô hình chung cho quá trình giấu và tách tin

Các tham số chính trong mô hình trên là $\{X, M, S, K, E, D\}$ trong đó [1]:

- X là vật chứa.
- M là thông tin cần giấu.
- S là vật chứa đã chứa tin.
- K là khóa.
- E là bộ nhúng thông tin.
- D là bộ tách thông tin.
- Quá trình nhúng thông tin là quá trình xử lý $E: X \times M \times K \rightarrow S$
- Quá trình tách thông tin là quá trình xử lý $D: S \times K \rightarrow M, X$

b) Các khái niệm trong mô hình giấu và tách tin

- Vật chứa X : Là các đối tượng được dùng làm môi trường để giấu tin như ảnh, âm thanh, video, văn bản,...

- Thông tin cần giấu 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).

- Khóa K : 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.

- Vật chứa tin S : là vật chứa đã chứa tin, về cơ bản 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 tiền 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 tiền mã hóa là thông tin đã mã hóa M' .

- Bộ 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.

- 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.

- Bộ tách thông tin: 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.

- Máy dò: Dùng để phát hiện có thông tin được giấu trong vật chứa hay không hoặc thông tin giấu còn nguyên vẹn hay không (thông tin giấu có thể bị sửa đổi do các lỗi trong kênh thông tin, các lỗi trong hoạt động xử lý tín hiệu hoặc do các vụ tấn công cố ý). Máy dò sử dụng các biện pháp như khoảng cách Hamming hoặc tương quan chéo giữa vật chứa hiện tại và bản gốc (trong trường hợp có sự hiện diện của nó).

- Bộ giải mã: dùng để phục hồi thông tin được giấu M . Nút này có thể bị bỏ qua.

1.1.2. Một số 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 tin. Vấn đề đặt ra là làm thế nào để thông tin này có thể trên 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 lợi dụng vào 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.

- **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 chỉ tiêu khác nhau như tính vô hình, tính bền vững.

- **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 bảo 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 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.

1.1.3. Lịch sử phát triển

Kỹ thuật giấu tin được phát triển thành hai lĩnh vực chính với những yêu cầu và tính chất khác nhau đó là giấu thông tin bí mật và thủy vân số. Giấu tin mật chủ yếu phục vụ cho mục đích liên lạc bí mật còn thủy vân số là việc nhúng thông tin mang ý nghĩa bảo vệ tính toàn vẹn của vật chứa [3].

Giấu tin mật: lĩnh vực giấu tin mật 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 ghi lại [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 ký 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.

Kỹ thuật thủy vân: lĩnh vực 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. 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.

1.1.4. 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 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 thực tế. Vì vậy, chủ sở hữu sản phẩm số luôn tìm kiếm các công nghệ bảo vệ quyền của mình. Lựa chọn đầu tiên là mật mã: Sản phẩm số được mã hóa trước khi gửi và khóa 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 thực sự 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 được gỡ bỏ 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. Thủy vân số đã được ứng dụng nhiều trong chống sao chép và bảo vệ bản quyền. 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 nhuận bút 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. Để giải quyết vấn đề này, nhiều kỹ thuật giấu tin khác nhau đã được phát triển. 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.

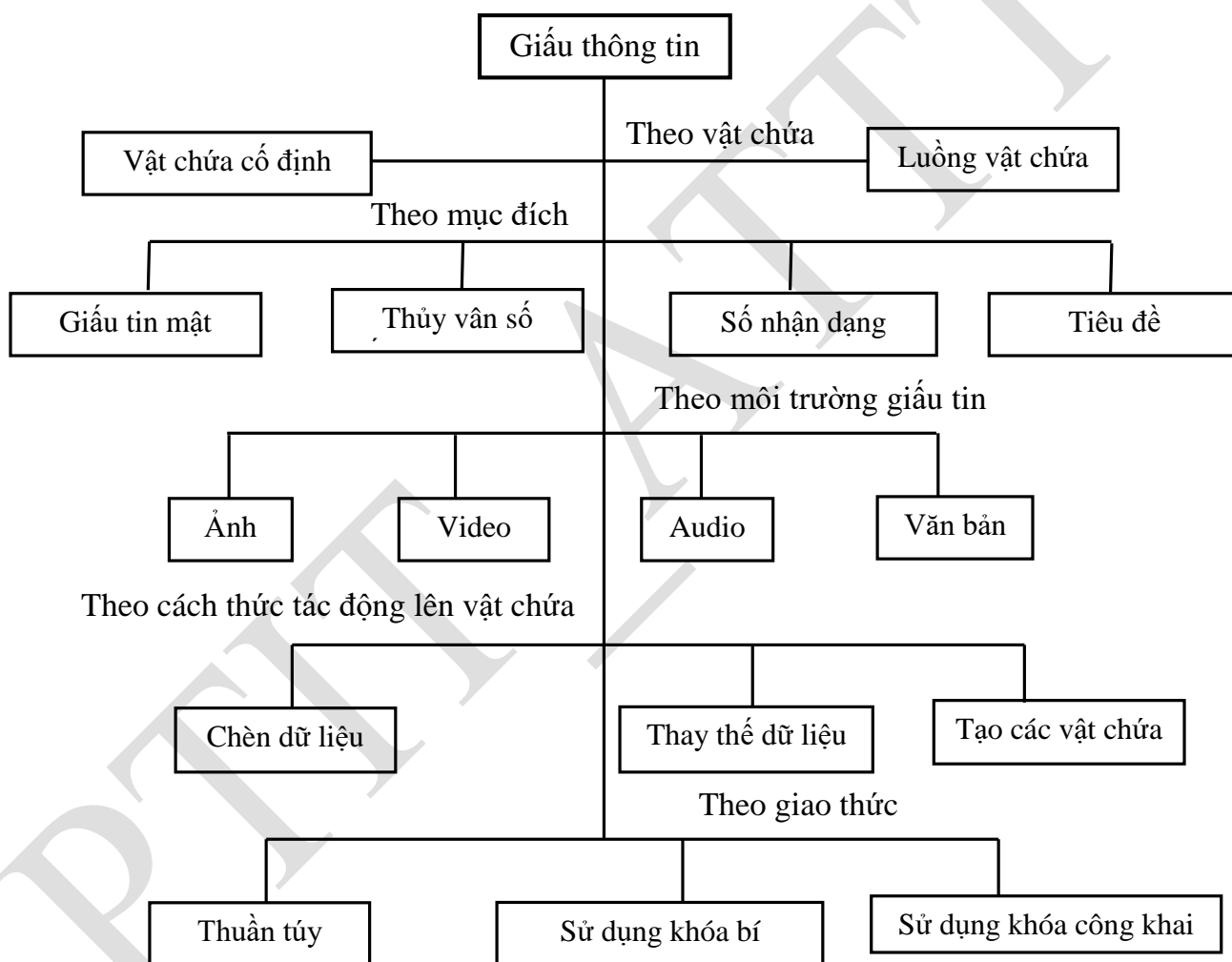
- Tính toàn vẹn thông tin (integrity): đảm bảo thông tin không bị thay đổi trong quá trình truyền tin hay khi có bất kì hành động nào tác động vào vật chứa tin; hoặc nếu có thay đổi thì sẽ bị phát hiện.

- 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

Trong thực tế kỹ thuật giấu tin nhằm hai mục đích chính là: bảo mật cho dữ liệu được đem giấu và bảo vệ cho chính đối tượng mang tin giấu. Hình 1.2 mô tả tổng quan về các kỹ thuật giấu tin đang được ứng dụng trong thực tế hiện nay [1, 2].



Hình 1.2. Phân loại các kỹ thuật giấu tin

Từ hình 1.2 có thể thấy rằng, 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, hãy cùng tìm hiểu về đặc điểm của từng phương pháp giấu tin.

1.2.1. Phân loại theo vật chứa

Trên hình 1.2 có thể thấy một số đặc điểm và tiêu trí phân loại theo phương pháp này như sau:

- **Luồng vật chứa:** Luồng vật chứa là các chuỗi bit liên tục. Thông điệp được nhúng vào trong thời gian thực, vì vậy bộ nhúng thông tin không được biết trước kích thước thông tin cần giấu cho dù kích thước vật chứa đủ để chứa và truyền toàn bộ thông tin cần giấu. Trong một vật chứa lớn, có thể nhúng vài 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 chen các bit đồng bộ hóa, tiêu đề gói tin vào trước các thông tin ẩn. Giấu tin với luồng vật chứa không có tính khả thi cao.

- **Vật chứa cố định:** Trong một vật chứa cố định thì kích thước và đặc điểm của thông tin cần giấu cần biết trước. Điều này trong thực tế đã mang lại nhiều lợi ích hơn. Vì vậy, các kỹ thuật giấu tin thường sử dụng vật chứa cố định. Vật chứa có thể được lựa chọn ngẫu nhiên hoặc áp đặt trước. Vật chứa được chọn tùy thuộc vào thông tin mật cần giấu. Vật chứa có thể được lựa chọn trước hoặc chọn ngẫu nhiên. Vật chứa chọn trước thường được sử dụng khi người cung cấp nghi ngờ vật chứa có khả năng tương thích ẩn và muốn ngăn chặn nó. Trong thực tế, hầu hết các ứng dụng thường lựa chọn giấu tin vào vật chứa được lựa chọn ngẫu nhiên.

1.2.2. Phân loại theo môi trường giấu tin

Theo môi trường đa phương tiện, giấu tin được chia thành:

- **Giấu tin trong ảnh:** 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: nhận thực thông tin, xác định xuyên tạc thông tin, bảo vệ bản quyền tác giả, giấu thông tin mật.

- **Giấu tin trong âm thanh:** là các phương pháp nhằm giấu thông tin vào môi trường âm thanh. Giấu tin trong âm thanh thường áp dụng các biện pháp và kỹ thuật nhằm 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. Hiện nay, giấu tin trong âm thanh cũng đang được quan tâm và ứng dụng trong thực tế.

- **Giấu tin trong video:** là các phương pháp nhằm giấu thông tin vào môi trường âm thanh hoặc hình ảnh. Giấu tin trong video cũng được quan tâm và được phát triển mạnh mẽ cho nhiều ứng dụng như điều khiển truy cập thông tin, nhận thực thông tin và bảo vệ bản quyền tác giả. Ví dụ như 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 nhúng thông tin vào môi trường văn bản. Giấu tin trong văn bản dạng văn bản khó thực hiện hơn do có ít các thông tin dư thừa.

1.2.3. Phân loại theo cách thức tác động lên vật chứa tin

Gồm 3 phương pháp tác động lên vật chứa tin:

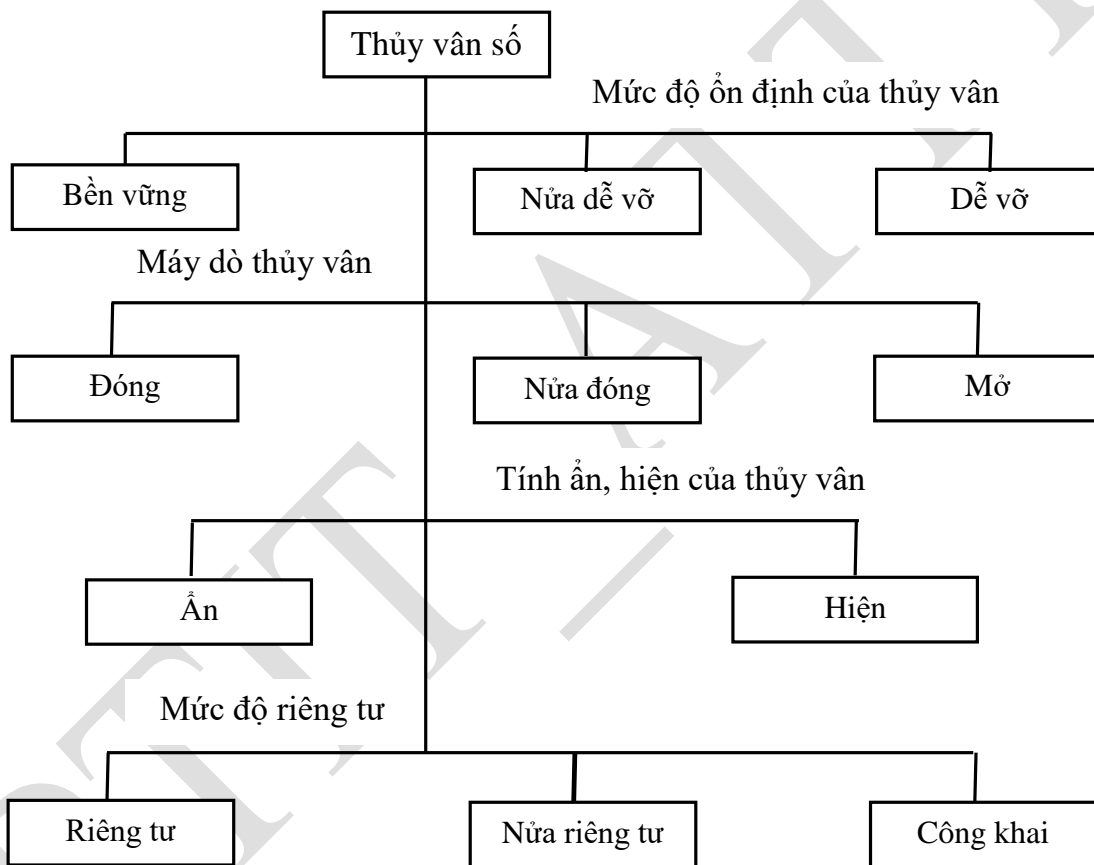
- Phương pháp chèn dữ liệu: là phương pháp này tìm các vị trí trong tệp để bị bỏ qua và chèn dữ liệu cần giấu vào, cách giấu này không làm ảnh hưởng tới sự thể hiện các tệp dữ liệu.
- Phương pháp thay thế: là phương pháp thay thế trực tiếp các phần tử của thông tin cần giấu vào các vị trí ít được chú ý và ít quan trọng nhất. Phương pháp này làm thay đổi vật chứa khá 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 tần số, thay thế các bit ít quan trọng, các kỹ thuật trải phổ, thống kê.
- Phương pháp tạo các vật chứa: Từ các thông điệp 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.

1.2.4. Phân loại theo mục đích sử dụng

Từ hình 1.2 thấy rằng, 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 (Steganography): 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, đảm bảo tính bí mật và vô hình của thông tin được giấu. 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 như là giấu các chữ ký vào vật chứa. Mục đích của nhúng tiêu đề là 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 (Watermarking): là phương pháp giấu thông tin (thủy vân) vào các vật chứa. Hình thức này nhằm đảm bảo tính toàn vẹn và xác thực của sản phẩm. Thủy vân là một thông tin nào đó mang ý nghĩa quyền sở hữu của tác giả đối với một sản phẩm, thông tin này chỉ tác giả đó có và được dùng làm minh chứng cho bản quyền sản phẩm. 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,... Tùy vào ứng dụng cụ thể mà người giấu tin sẽ áp dụng những phương pháp thủy vân số khác nhau. 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

Để hiểu rõ hơn về các phương pháp thủy vân số trên hình 1.3 hãy cùng tìm hiểu các định nghĩa cho các kỹ thuật này.

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: thủy 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, toàn 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. Tùy thuộc vào đầu vào của máy dò, hệ thống thủy vân được chia thành:

- Hệ thống đóng: đầu vào cần vật chứa gốc (chưa có thủy vân) 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:

○ 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: đầu vào không cần vật chứa gốc X nhưng cần bản sao của thủy vân M .

+ 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:

+ 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 thủy 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 thủy 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 thủy vân ra khỏi vật chứa tin. 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 tin. 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 nhúng 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 (xem mục 1.4.3. Kiểm soát sao chép).

1.2.5. Phân loại theo theo giao thức

a) Giấu tin thuần túy

Giấu tin thuần túy là hệ thống giấu thông tin không yêu cầu phải trao đổi trước một số thông tin bí mật. Người giấu tin và người tách tin cùng thực hiện một thuật toán nhúng 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, phương tiện 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 phương tiện chứa.

b) Giấu tin sử dụng khóa bí mật

Giấu tin sử dụng khóa bí mật là hình thức người gửi chọn phương tiện chứa thông tin, sử dụng khóa bí mật, tiến hành nhúng thông tin vào phương tiện chứa đó. Khóa có thể được chọn bằng một số phương pháp như:

- Có thể dùng một số đặc tính của chính phương tiện chứa làm khóa hoặc dùng hàm băm tính toán các giá trị này để làm khóa.
- Có thể chọn các thành phần quan trọng trong phương tiện chứa để làm khóa. Các thành phần đó nếu bị thay đổi sẽ ảnh hưởng nghiêm trọng tới phương tiện chứa và có thể nhận ra được.
- Người nhận cũng tính hàm băm trên chính các giá trị này để lấy khóa giải mã tách thông tin.

c) Giấu tin sử dụng khóa công khai

Yêu cầu có 2 khóa: khóa bí mật và khóa công khai. Khóa công khai được dùng trong quá trình giấu thông tin. Khóa bí mật chỉ có ng 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 hàm 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 chứa.

1.3. Một số ứng dụng của kỹ thuật giấu tin

1.3.1. Lấy dấu vân tay (*fingerprinting*)

a) Giới thiệu

Lấy dấu vân 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 với các đối tượng khác [2, 4]. Các kỹ thuật gán 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.

b) Ví dụ lấy dấu vân tay bất đối xứng trong mua bán hình ảnh số

Các dấu vân tay ngăn cản mọi người sao chép dữ liệu số bất hợp pháp bằng cách: khi có bản sao được phân phối lại bất hợp pháp, thì người bán có thể xác định người mua ban đầu của bản sao này. Thông thường, các chương trình lấy dấu vân tay là 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 có tình vụ không 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. Chi tiết ứng dụng này được mô tả tại tài liệu [4].

1.3.2. Xác thực nội dung (content authentication)

Cách tiếp cận phổ biến cho vấn đề này là 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 việc xác thực cục bộ: nếu một hình ảnh được chia thành các khối và mỗi khối có dấu hiệu xác thực riêng được nhúng trong nó. Người quản 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. Hãy tưởng tượng 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 biến số xe hơi. 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)

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 thủy 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 [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. Xét đến hệ thống chống sao chép đĩa DVD có các định nghĩa sau:

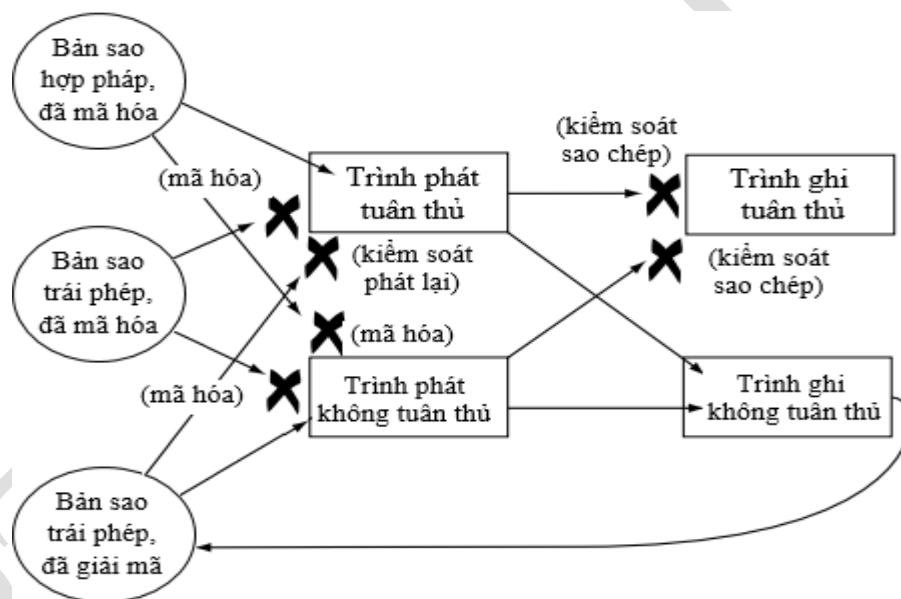
- Trình phát tuân thủ: là trình phát chỉ phát bản sao hợp pháp.
- Trình ghi tuân thủ: là trình ghi không cho phép sao chép bản sao có thủy vân chống copy (never-copy).

- 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. Ý tưởng của kiểm soát sao chép bằng kỹ thuật giấu tin 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 never-copy.
 - 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).

- Nếu đĩa DVD là một bản sao trái phép đã được giải mã sẽ:
 - + 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.



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

Do đó, 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).
- 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)

Đây là ứng dụng cơ bản nhất của kỹ thuật thủy văn số. Một thông tin nào đó mang ý nghĩa quyền sở hữu tác giả sẽ được nhúng vào trong các sản phẩm. Thủy văn 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 thủy văn 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 thủy văn phải tồn tại bền vững cùng với sản phẩm muốn bảo thủy văn này mà không được phép của người chủ sở hữu thì chỉ còn cách là phá hủy sản phẩm đó.

1.3.5. Một số ứng dụng khác

- Truyền thông tin mật: Liên lạc bí mật giữa hai bên tham gia truyền thông mà không bị bên thứ ba phát hiện. Xây dựng kênh truyền thông bí mật [2, 3, 5].

- Ứng dụng xấu: Tội phạm mạng sử dụng các kỹ thuật giấu tin mật để tạo Malware (phần mềm độc hại). Một trong cách phổ biến nhất là sử dụng các tệp đa phương tiện làm môi trường để giấu các mã độc. Một trong các kỹ thuật phổ biến nhất là sử dụng ảnh kỹ thuật số để che giấu cài đặt phần mềm độc hại hoặc một tập tin cấu hình hay lưu trữ trực tiếp toàn bộ mã độc hại. 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 chiết xuất các bit quan trọng nhất từ mỗi pixel của hình ảnh để tái tạo lại một URL được nhúng trước đó để tải tập tin cấu hình của nó.

- + Các phần mềm độc hại như Ransomware 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.

- + 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. Câu hỏi ôn tập

Câu 1. Hãy trình bày 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. Hãy trình bày về ứng dụng của giấu tin trong bảo vệ bản quyền tác giả?
- Câu 4. Hãy trình bày về ứng dụng của giấu tin trong kiểm soát sao chép?
- Câu 5. Hãy trình bày về ứng dụng của giấu tin trong xác thực nội dung?
- Câu 7. Hãy trình bày về ứng dụng của giấu tin trong lấy dấu vân tay?
- Câu 8. Hãy trình bày về khái niệm về thủy vân bền vững? Hãy lấy ví dụ minh họa của thủy vân bền vững?
- Câu 9. Hãy trình bày về khái niệm về thủy vân dễ vỡ? Hãy lấy ví dụ minh họa của thủy vân dễ vỡ?
- Câu 10. Hãy trình bày về khái niệm về thủy vân riêng tư? Hãy lấy ví dụ minh họa của thủy vân riêng tư?
- Câu 11. Hãy trình bày về khái niệm của giấu tin mật và thủy vân số? Hãy nêu vai trò và tầm quan trọng của kỹ thuật giấu tin trong an toàn thông tin.

CHƯƠNG 2: GIẤU TIN TRONG ẢNH

Chương 2 cung cấp các kiến thức về kỹ thuật giấu tin và tách tin trong ảnh tĩnh. Một số phương pháp giấu tin trong ảnh tĩnh hiện nay bao gồm: LSB, hoán vị giả ngẫu nhiên, kỹ thuật biến đổi DCT, DWT... Bên cạnh đó, trong chương 2 bài giảng còn cung cấp một số phương pháp phát hiện ảnh tĩnh có giấu tin.

2.1. Một số vấn đề trong giấu tin trong ảnh

2.1.1. Khái niệm và yêu cầu của kỹ thuật giấu tin 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 cùng với dữ liệu ảnh 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. Đây chính là lợi thế từ sự hạn chế về cảm nhận hình ảnh của con người. Kỹ thuật giấu tin trong ảnh có ưu điểm là giấu được lượng lớn thông tin mà vẫn đảm bảo được các tính chất ban đầu của ảnh. Thông tin trong ảnh được giấu một cách vô hình như cách 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 mà 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. Tài liệu sau đó được truyền trực tiếp qua máy fax hoặc lưu truyền trên mạng.

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 bên cạnh việc 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].

2.1.2. Một số định dạng ảnh

Hiện nay có nhiều loại định dạng ảnh khác nhau có thể được lựa chọn để giấu tin. Tuy nhiên, cần lưu ý là mỗi định dạng ảnh sẽ có những đặc tính khác nhau. Chính vì vậy để đảm bảo được những yêu cầu và tính chất của giấu tin trong ảnh thì các chuyên gia thường rất quan tâm đến quá trình lựa chọn định dạng ảnh. Trong bài giảng sẽ trình bày một số định dạng ảnh chính đang được sử dụng phổ biến hiện nay.

a) Định dạng ảnh BMP [6]

BMP được biết đến với tên tiếng Anh khác là Windows bitmap, là một định dạng tập tin hình ảnh khá 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. Định dạng ảnh BMP có khả năng lưu trữ hình ảnh kỹ thuật số hai chiều cả đơn màu và 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 pixel
Mặt nạ thêm bit	12 hoặc 16 byte	Xác định định dạng pixel.
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

Một hình ảnh BMP khi không nén là một ma trận điểm ảnh. 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).

b) Định dạng ảnh PNG

PNG (Portable NetWork Graphics) là một dạng hình ảnh sử dụng phương pháp nén dữ liệu mới – 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), hình ảnh xám (có hoặc không có kênh alpha) và hình ảnh RGB / RGBA không có bảng màu đầy đủ. Các giá trị trong phần tiêu đề của định dạng ảnh PNG cho 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 tin 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

Theo sau tiêu đề tập tin PNG là một chuỗi các chunk (là một đoạn thông tin được sử dụng trong nhiều định dạng đa phương tiện), mỗi một chunk truyền tải thông tin nhất định về hình ảnh. Có hai loại chunk: một là chunk quan trọng, hai là chunk phụ trợ. Một bộ giải mã có khả năng đọc các chunk quan trọng và hiển thị tệp PNG. Các chunk 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 chunk quan trọng bao gồm IHDR, PLTE, IDAT, IEND. Giá trị của các IHDR, PLTE, IDAT, IEND được mô tả trong tài liệu [7].

c) 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. Ưu điểm của ảnh định dạng JPEG là 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
SOF _n	0xFF, 0xC _n	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

2.1.3. Phân loại kỹ thuật giấu tin trong ảnh

Giấu tin trong ảnh hiện nay được ứng dụng rộng rãi trong thực tế và trong nhiều lĩnh vực khác nhau như trong các chương trình ứng dụng, các phần mềm, hệ thống giấu tin trong đa phương tiện; trong các ứng dụng bảo mật thông tin: xác thực thông tin, xác định xuyên tạc thông tin, bảo vệ bản quyền tác giả, kiểm soát truy cập, giấu thông tin mật,... Một số nhóm kỹ thuật giấu tin trong ảnh đang được ứng dụng hiện nay như sau [1, 2, 5, 10, 14]:

a) Giấu tin trên miền không gian ảnh

Giấu tin trên miền không gian ảnh đây là kỹ thuật giấu tin tương đối phổ biến hiện nay. Với kỹ thuật này thông tin sẽ được giấu vào các điểm ảnh. 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. Một số thuật toán và kỹ thuật thường được sử dụng để giấu tin trong miền không gian như:

- 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.

b) 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 sử 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.

c) Một số hướng tiếp cận khác

Hướng tiếp cận giấu tin trong ảnh trên miền không gian và miền tần số là hai hướng tiếp cận chính. Tuy nhiên, hiện nay ngoài hai hướng phổ biến trên thì còn có một số bài báo khoa học và các công trình nghiên cứu đã đề xuất một số hướng tiếp cận khác như:

- Kỹ thuật Cox;
- Kỹ thuật trải phổ chuỗi trực tiếp.

2.2. Phương pháp giấu tin trên miền không gian

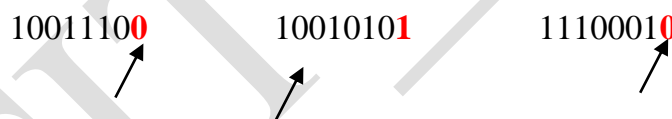
2.2.1. Phương pháp thay thế

a) Tổng quan về phương pháp thay thế LSB

Phương pháp thay thế LSB là phương pháp mà thông tin sẽ được thay thế vào các bit có trọng số thấp nhất trong mỗi điểm ảnh [10]. Bit có trọng số thấp là bit có ảnh hưởng ít nhất tới việc quyết định tới màu sắc của mỗi điểm ảnh. Vì vậy, khi thay đổi bit ít quan trọng của một điểm ảnh thì màu sắc của mỗi điểm ảnh mới sẽ tương đối gần với điểm ảnh ban đầu. 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,...

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

10011100 10010101 11100010



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) Phương pháp giấu tin và tách tin trên k bit LSB

+ Phương pháp giấu tin

- Đầu vào của phương pháp bao gồm:
 - o Ảnh gốc C .
 - o 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: $C = \{x_{ij} | 0 \leq i \leq M_c, 0 \leq j \leq N_c, x_{ij} = \{0, 1, 2, \dots, 255\}\}$

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:

$$M = \{m_i | 0 \leq i < n, m_i \in \{0, 1\}\}$$

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. Được ảnh mới đã giấu tin.

+ 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 minh họa cho phương pháp giải mã như sau: 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 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) Đánh giá phương pháp LSB

- *Ưu điểm:*

- Chất lượng hình ảnh sau giấu tin hầu như không bị ảnh hưởng.
- Kỹ thuật LSB đơn giản, dễ cài đặt và phát huy hiệu quả tốt trong nhiều ứng dụng.

- *Nhược điểm:*

- Tính bền vững thấp; thông tin mật dễ bị thay đổi do sự tác động vào hình ảnh.
- Phát hiện thông tin dễ dàng vì thuật toán đơn giản. 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. Phương thức Seed thông qua phép logarithm rời rạc để chọn ra các dãy pixel 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 Seed.

2.2.2. Phương pháp hoán vị giả ngẫu nhiên

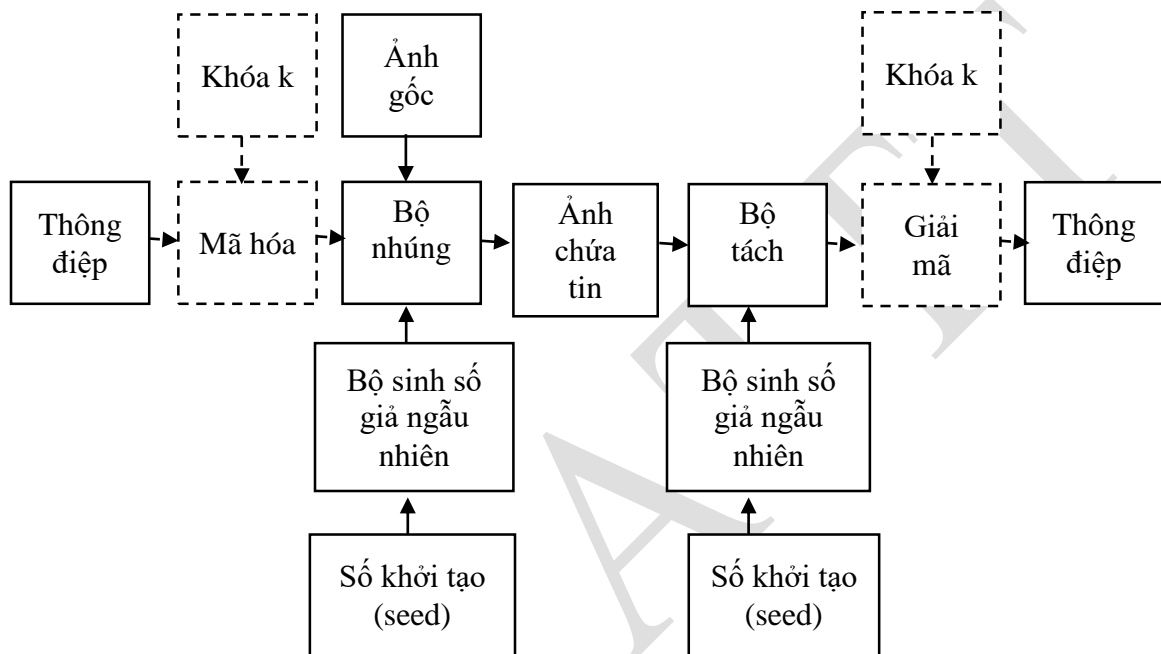
a) Tổng quan về phương pháp hoán vị giả ngẫu nhiên

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, nhưng dễ bị tấn công vét cạn hoặc nhận dạng tự động.

Ý tưởng của giải pháp hoán vị giả 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 nhúng 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 điệp được giấu. Chính vì vậy, phương pháp hoán vị giả ngẫu nhiên sẽ rất khó thực hiện.

Để giải quyết vấn đề này, các chuyên gia đề xuất giải pháp là hoán vị giả ngẫu nhiên. Theo đó, hoán vị giả ngẫu nhiên sẽ vẫn dựa trên giải pháp hoán vị giả ngẫu nhiên nhưng vị trí các

bit được lựa chọn để nhúng thông điệp 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. Hình 2.2 dưới đây 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 nhúng và tách tin của phương pháp 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), là thuật toán sinh ra chuỗi các số có các thuộc tính gần như thuộc tính của chuỗi số ngẫu nhiên [11, 12]. Chuỗi sinh ra từ bộ sinh số giả ngẫu nhiên không thực sự là ngẫu nhiên, do nó hoàn toàn được xác định từ giá trị khởi đầu, được gọi là nguồn (seed) của nó (mà giá trị này có thể hoàn toàn là ngẫu nhiên). Mặc dù chuỗi giả ngẫu nhiên này gần giống với chuỗi được sinh ra bằng bộ sinh số ngẫu nhiên từ phần cứng, bộ sinh số giả ngẫu nhiên có vai trò rất quan trọng trong thực tế vì tốc độ trong quá trình tạo số và khả năng tái sử dụng của nó.

Để hiểu rõ hơn về bộ sinh số giả ngẫu nhiên, bài giảng đi vào 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:

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

Sau đó tính giá trị $M = p * q$ và lựa chọn một nhân (seed - 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:

$$x_{n+1} = x_n^2 \bmod M$$

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

b) Kỹ thuật giấu tin bằng phương pháp hoán vị giả ngẫu nhiên

Theo sơ đồ tổng quan về quá trình giấu và tách tin, để thực hiện giấu tin và giải mã, 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 điệp được mã hóa thì hai bên cũng cần thống nhất thuật toán mã hóa, giải mã và gửi khóa qua kênh truyền an toàn.

+ Thuật toán giấu tin

Bước 1: Thông điệp 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 điệp

+ Thuật toán tách tin

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.

c) Đánh giá về phương pháp hoán vị giả ngẫu nhiên

- Ưu điểm

- Độ an toàn cao: 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.

- Nhược điểm:

- Dễ xảy ra việc xung đột trong quá trình nhúng khi chu kỳ 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

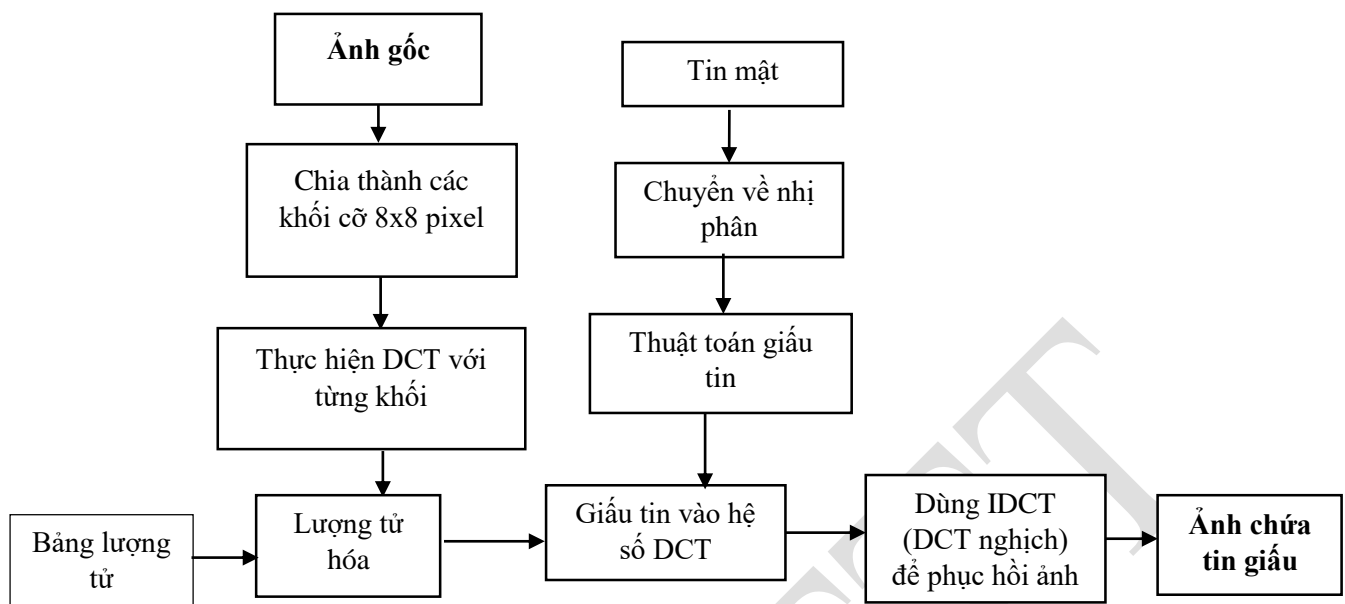
- Ảnh sẽ bị thay đổi giá trị rất nhiều do các bit thông điệp được giấu vào các bit bất kì chứ không phải chỉ bit LSB. Điều này dẫn đến kẻ tấn công dễ dàng phát hiện ảnh đang chứa tin chỉ cần nhìn qua bằng mắt thường. Để giải quyết nhược điểm này, trong thực tế các chuyên gia thường kết hợp giữa kỹ thuật 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 nhúng thông tin và các vị trí vừa tìm được.

2.3. Phương pháp giấu tin trên miền tần số

2.3.1. Phương pháp biến đổi miền tần số DCT

a) Tổng quan về phương pháp DCT

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 đổi cosine rời rạc (Discrete Cosine Transform- DCT). Phương pháp DCT trong 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: dữ liệu của ảnh con tập trung vào một phần nhỏ các hệ số hàm truyền.



Hình 2.3. Sơ đồ tổng quan về quá trình giấu tin trong ảnh sử dụng phương pháp biến đổi DCT

Từ sơ đồ 2.3 thấy được, quá trình giấu tin và tách trong ảnh sử dụng biến đổi DCT gồm các bước sau [1, 2, 5, 10, 14]:

- Biến đổi DCT;
- Lượng tử hóa;
- Giấu tin vào hệ số DCT;
- Phục hồi ảnh.

Tiếp theo bài giảng sẽ trình bày chi tiết về các các quy trình biến đổi này.

b) Biến đổi DCT

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 block các tín hiệu chói (Y) và 2; 4 hoặc 8 block các mẫu tín hiệu màu (Cr, Cb). Tất cả các block có cùng kích thước và mỗi block có kích thước 8 x 8 pixel và biểu diễn các mức xám của 64 điểm ảnh [2, 5, 10, 14]. 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 8*8 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.

+ *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 sau:

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

Hàm biến đổi DCT ngược (một chiều):

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

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.

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

+ 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 [7]:

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

Trong đó:

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

$F(u, v)$ là các hệ số của khối DCT 8x8

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

Phương trình trên là kết quả của hai phương trình 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 block 8*8.

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

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 bloc ảnh 8*8 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 sau:

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

Để hiểu rõ hơn về vấn đề biến đổi DCT, ví dụ dưới đây sẽ trình bày quy trình biến đổi ảnh từ miền không gian sang miền tần số.

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

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

Bước 1: Tiền xử lý ảnh: Trừ giá trị của các pixel 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:

$$D = TMT'$$

Ma trận T được định nghĩa theo công thức:

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

Với i là số hàng còn j là số cột

N là giá trị của số pixel tối đa. Vì đầu vào ở đây là khối 8x8 pixel 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.

c) 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 $0 \leq u, v \leq 7$. 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.

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

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.

Ví dụ với ma trận D thu được từ phép biến đổi DCT. Với ma trận lượng tử Q cho trước. Trong ví dụ này chọn ma trận lượng tử hóa là Q_{50}

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

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.

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

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.

d) Thuật toán giấu tin vào hệ số DCT

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.

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

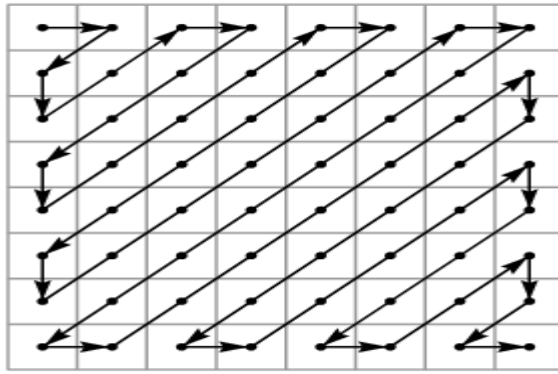
Đầu ra:

- Ảnh có chứa thông điệp.

Lưu ý trong quá trình giấu tin sử dụng thuật toán LSB như sau

-Ảnh dùng để giấu tin sẽ có kích thước rất lớn và bao gồm nhiều khối 8×8 pixel 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 (vì sẽ có những điểm ảnh xấu – làm việc giấu nhiều hơn một kí tự vào ảnh là không thể).

-Vị trí LSB: 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 *zigzag* 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

Như thấy thì ở trong trường hợp này ma trận C_{50} trải thẳng xong thì 3 pixel 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 pixel này bằng 3 bit của bản rõ ban đầu (010). Kết quả giấu tin bằng thuật toán LSB như sau:

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

e) Phục hồi ảnh.

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

$$R_{ij} = Q_{ij} * C_{ij}$$

Trong đó Q_{ij} là ma trận lượng tử được sử dụng ở trên (Q_{50})

C_{ij} là kết quả của ma trận lượng tử đã được giấu tin ở trên (C_{50LSB})

Kết quả thu được là ma trận điểm ảnh R như sau:

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

Cuối cùng thực hiện IDCT ma trận R sẽ thu được ảnh mới:

$$N = \text{round}(T'R T) + 128$$

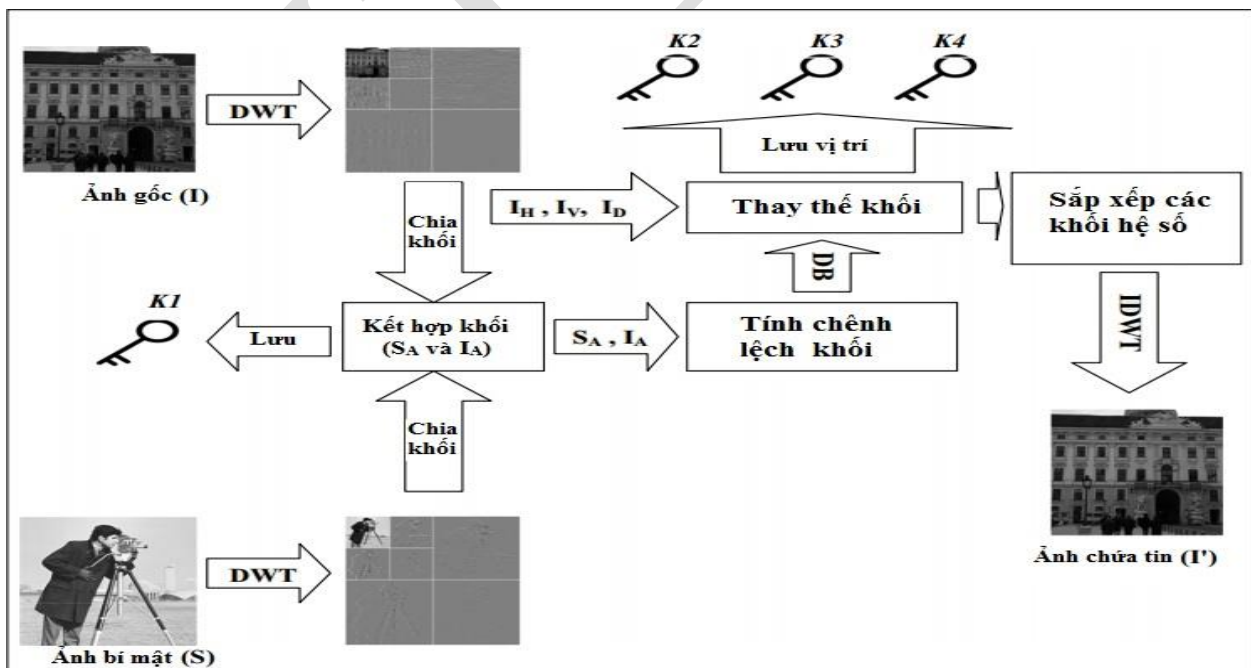
$$N_{\text{new}} = \begin{bmatrix} 151 & 129 & 124 & 114 & 119 & 130 & 123 & 130 \\ 198 & 181 & 127 & 149 & 161 & 137 & 148 & 119 \\ 261 & 176 & 175 & 158 & 175 & 185 & 111 & 119 \\ 235 & 208 & 125 & 176 & 193 & 137 & 148 & 97 \\ 197 & 126 & 156 & 145 & 163 & 183 & 118 & 146 \\ 123 & 142 & 105 & 151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

Nếu so sánh 2 ma trận điểm ảnh N và N_{new} thì sẽ thấy có rất ít thông tin bị thay đổi giữa N và N_{new} .

2.3.2. Phương pháp biến đổi DWT

2.3.2.1. Tổng quan về phép biến đổi DWT

Kỹ thuật biến đổi Wavelet rời rạc (Discrete Wavelet Transformation - DWT) là ứng dụng mới trong các ứng dụng của wavelet. 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 nhúng tin. DWT cung cấp những ưu điểm khắc phục hạn chế của hai phép biến đổi DCT và DFT. Hạn chế của các kỹ thuật dựa trên biến đổi DCT tạo ra các vấn đề giả tạo (artifact problems), còn các kỹ thuật biến đổi dựa trên DFT chỉ cung cấp thông tin về tần số mà không cung cấp thông tin về thời gian. Với các kỹ thuật dựa trên DWT, DWT cung cấp cả thông tin về thời gian cũng như thời gian, trái ngược với DFT; DWT cũng cung cấp sự đầm nén năng lượng tốt hơn so với DCT.



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

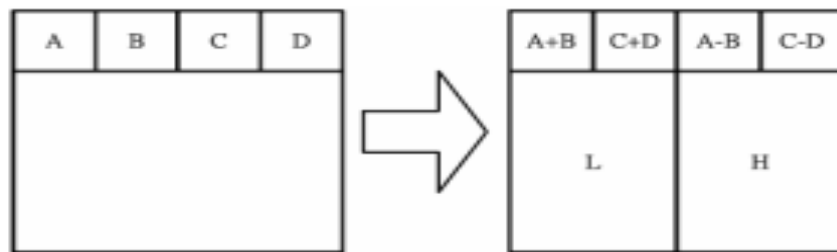
Mục đích của giải thuật nhằm giấu tin vào trong các hệ số tương ứng các ảnh phụ của ảnh gốc bằng cách thay thế các khối điểm ảnh trong ảnh phụ lưu hệ số bằng các khối lưu sự chênh lệch khối giữa ảnh gốc và ảnh bí mật. Từ hình 2.5 có thể thấy rằng các bước tiến hành trong kỹ thuật giấu tin trong ảnh sử dụng kỹ thuật biến đổi DWT như sau [1, 5, 10, 14, 15]:

- + Biến đổi DWT;
- + Chia khối (Blocking);
- + Kết hợp khối (Matching);
- + Tính chênh lệch khối (Difference Blocks Computation);
- + Thay thế khối (Block Replacement);
- + Sắp xếp các khối hệ số (Rearrangement of Coefficients Blocks).
- + Biến đổi DWT ngược

2.3.2.2. Quy trình giấu tin

a) Biến đổi DWT

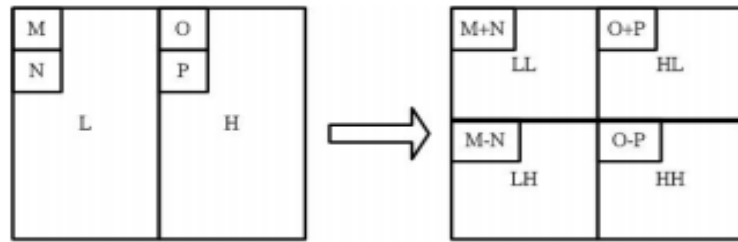
+ Bước 1: Thực hiện quét các điểm ảnh từ trái sang phải theo chiều ngang. Sau đó thực hiện phép cộng và phép trừ trên các điểm ảnh lân cận. Lưu trữ tổng ở bên trái và hiệu ở bên phải, như hình 2.6.



Hình 2.6. Quét theo chiều ngang

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 như hình 2.7.



Hình 2.7. Quét theo chiều dọc

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.



Hình 2.8. Hình ảnh gốc so với ảnh đã biến đổi DWT

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:

- 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:

- 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

Lưu ý là: Các ảnh phụ S_A , S_H , S_V , S_D được phân chia thành các khối không chồng nhau. Để hiểu rõ hơn về quá trình biến đổi DWT xét ví dụ sau.

Đầu vào: Với ảnh chứa I dưới dạng ma trận điểm ảnh 8×8 như sau:

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

Ảnh bí mật S dưới dạng ma trận 4x4 như sau:

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

Đầu ra: 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

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

+ Biến đổi chiều ngang

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

+ 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

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

b) Chia khối (Blocking)

Mục đích của chia khối: thuật toán thực hiện thay đổi và biến đổi theo đơn vị từng khối ảnh vậy nên cần thực hiện chia ảnh theo từng khối.

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

$$S_A = \{B_{SAi}, 1 \leq i \leq S_{An}\}$$

$$I_A = \{B_{IAj}, 1 \leq j \leq I_{An}\}$$

$$I_H = \{B_{IHk}, 1 \leq k \leq I_{Hn}\}$$

$$I_V = \{B_{IVl}, 1 \leq l \leq I_{Vn}\}$$

$$I_D = \{B_{IDp}, 1 \leq p \leq I_{Dn}\}$$

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 .

Để hiểu rõ hơn về quá trình biến đổi của quá trình chia khối. Hãy cùng xem xét ví dụ sau:

Với đầu vào là các ảnh phụ S_A , I_A , I_H , I_V , I_D thu được ở bước biến đổi DWT. Đầu ra: 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} :

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

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

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

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

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

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

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

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

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

c) Kết hợp khối (Matching)

Mục đích của kết hợp khối: quá trình giấu tin thực hiện thay thế các khối ảnh, vì vậy 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 Root Mean Square Method (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.

Ví dụ: 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 (Root Mean Square Error) [15]. Các giá trị RMSE của từng cặp tính được như sau

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

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

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

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

$RMSE(B_{SA}, B_{IA2})$ có giá trị thấp nhất, vậy nên khối B_{IA4} là khối phù hợp nhất với B_{SA} . Khóa K_1 lưu giá trị 4 - vị trí khối B_{IA4}

d) Tính chênh lệch khối (Difference Blocks Computation)

Thực hiện tính giá trị chênh lệch khối DB_i giữa khối B_{SAi} và khối phù hợp nhất B_{IAj} theo công thức sau:

$$DB_i = B_{SAi} - (\min_{1 \leq j \leq I_{An}} B_{IAj})$$

Mục đích của 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 . Ví dụ với đầu vào là các khối B_{SAi} và các khối B_{IAj} phù hợp nhất tương ứng thu được ở bước kết hợp khối 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:

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

e) Thay thế khối (Block Replacement)

Mục đích của thay thế khối: thuật toán thực hiện giấu tin vào trong 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 sau:

$$B_{tCH} = \min_{1 \leq k \leq IHn} (RMSE (DB_i, B_{IHk}))$$

$$B_{tCV} = \min_{1 \leq l \leq IVn} (RMSE (DB_i, B_{IVl}))$$

$$B_{tCD} = \min_{1 \leq p \leq IDn} (RMSE (DB_i, B_{IDp}))$$

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.

Đầu vào: Các khối chênh lệch DB_i , các khối của ảnh phụ I_H , I_V , I_D

Đầu ra: 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 .

Các bước tiến hành như sau:

- Thực hiện tính khối phù hợp nhất với khối DB trong các khối B_{IH} :

$$RMSE (DB, B_{IH1}) = 98.710$$

$$RMSE (DB, B_{IH2}) = 82.058$$

$$RMSE (DB, B_{IH3}) = 113.756$$

$$RMSE (DB, B_{IH4}) = 94.211$$

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

- 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

- Thực hiện tính khối phù hợp nhất với khối DB trong các khối B_{ID}

$$RMSE (DB, B_{ID1}) = 86.803$$

$$RMSE (DB, B_{ID2}) = 105.525$$

$$RMSE (DB, B_{ID3}) = 130.398$$

$$\text{RMSE}(\text{DB}, \text{B}_{\text{ID}4}) = 120.361$$

Vậy: Khối $\text{B}_{\text{ID}1}$ phù hợp với DB nhất trong các khối của I_D

-Tìm khối phù hợp nhất với khối DB trong 3 khối $\text{B}_{\text{IH}2}$, $\text{B}_{\text{IV}4}$, $\text{B}_{\text{ID}1}$ vừa tìm được. Từ các kết quả trên thấy rằng: Khối $\text{B}_{\text{IV}4}$ phù hợp nhất với $\text{RMSE}(\text{DB}, \text{B}_{\text{IV}4}) = 79.251$ vì kết quả thấp nhất.

Kết luận: khóa K_3 lưu cặp giá trị (1, 4) tương ứng $i=1$ và $k=4$.

Thực hiện thay thế DB vào vị trí $\text{B}_{\text{IV}4}$, $\text{B}_{\text{IV}4}$ thu được $\begin{bmatrix} -109 & 043 \\ -44 & 151 \end{bmatrix}$

f) Sắp xếp các khối hệ số

Sau khi thực hiện thay thế các khối, sắp xếp lại các khối theo đúng thứ tự và khôi phục lại ảnh qua phép biến đổi DWT ngược để thu được ảnh chứa tin. Ví dụ: Đầu vào: Các khối hệ số $\text{B}_{\text{IH}k}$, $\text{B}_{\text{IV}l}$, $\text{B}_{\text{ID}p}$ của ảnh phụ I_H , I_V , I_D sau khi giấu khối chênh lệch bằng cách thay thế. Đầu ra: Các ảnh phụ được sắp xếp theo đúng vị trí thứ tự các khối.

Vì chỉ thực hiện giấu DB vào một khối là $\text{B}_{\text{IV}4}$ nên ví dụ chỉ trình bày phân sắp xếp cho ảnh I_V tương ứng:

Các khối của ảnh phụ I_V sau khi giấu:

043 -18	000 013	018 -44	-109 043
115 -44	040 000	-08 -39	-44 151
$\text{B}_{\text{IV}1}$	$\text{B}_{\text{IV}2}$	$\text{B}_{\text{IV}3}$	$\text{B}_{\text{IV}4}$

Ảnh phụ I_V sau khi đưa về đúng vị trí:

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

g) 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

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

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

2.3.2.3. Quy trình tách tin

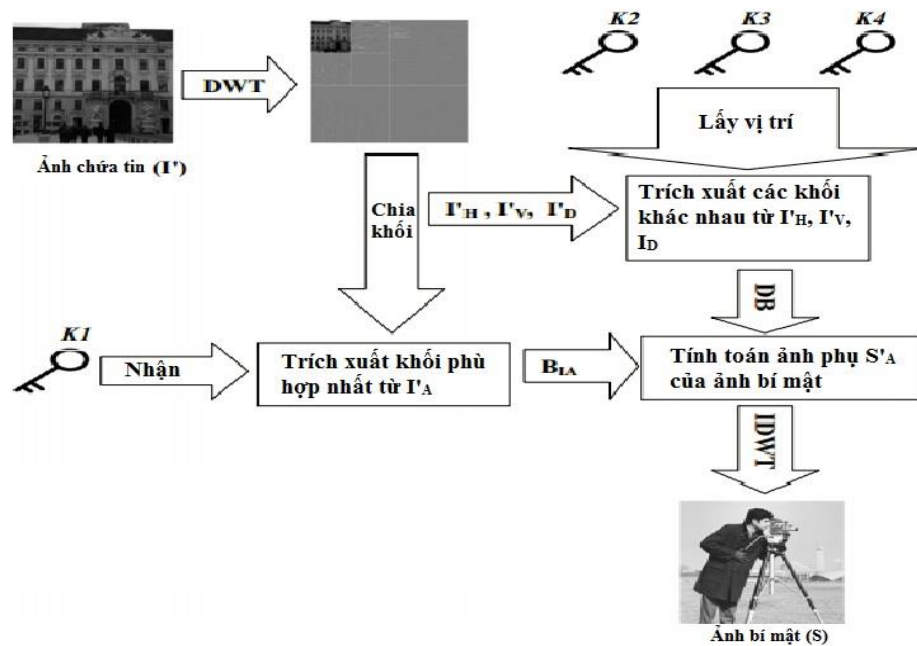
Từ sơ đồ tách tin được mô tả trong hình 2.6 có thể thấy được các bước chính của quá trình tách tin trong kỹ thuật biến đổi DWT như sau [15]:

- 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 4×4 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:

$$B_{SAi} = B_{IA'j} - DB'_i, \forall i = 1, \dots, S_{An} \text{ và } j = 1, \dots, I'_{An}$$

- 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 2.9. Mô hình tách tin trong kỹ thuật DWT

2.4. Phương pháp phát hiện giấu tin trong ảnh

Phương pháp phát hiện giấu tin trong ảnh là kỹ thuật phát hiện sự tồn tại của thông tin ẩn giấu trong ảnh. Mục đích của các phương pháp phát hiện giấu tin trong ảnh là phát hiện ra ảnh có mang thông tin và tìm cách lấy ra thông tin mật đó hoặc làm mất tính toàn vẹn của thông tin đó. Có nhiều phương pháp và kỹ thuật khác nhau để có thể phát hiện ra ảnh có giấu tin. Một số phương pháp cơ bản để phát hiện ảnh có giấu tin đang được biết đến hiện nay như sau [5, 10, 16]:

a) Phân tích trực quan

Phân tích trực quan là kỹ thuật dựa vào quan sát giữa ảnh gốc và ảnh chứa giấu tin để phát hiện ra sự khác biệt giữa hai ảnh. Sự khác biệt này là căn cứ đưa ra vấn đề nghi vấn ảnh có giấu tin hay không. Với phương pháp phân tích này thường khó phát hiện với ảnh có độ nhiễu cao và kích cỡ lớn. Phương pháp phát hiện giấu tin trong ảnh thuộc dựa vào kỹ thuật phân tích trực quan nổi tiếng là kỹ thuật phát hiện giấu tin dựa trên dịch chuyển Histogram. Kỹ thuật này là kỹ thuật phân tích tương quan biểu đồ tần số sai khác của ảnh. Kỹ thuật này được đề xuất bởi Tao Zhang và Xijian Ping. Các tác giả cho rằng, tồn tại sự khác biệt giữa biểu đồ tần số sai khác của ảnh bình thường và ảnh thu được sau khi đảo các bit trên miền LSB của ảnh. Đây là phương pháp đơn giản và kết quả thường không đáng tin cậy. Phương pháp này đòi hỏi phải có ảnh gốc để đối chiếu. Tuy nhiên, trong thực tế thì không phải lúc nào cũng có ảnh gốc để đối chiếu và so sánh.

b) Phân tích theo dạng ảnh

Phương pháp phân tích theo định dạng ảnh thường dựa vào các dạng ảnh bitmap hay là ảnh nén để nhận biết kỹ thuật giấu. Một số ảnh được lưu dưới dạng ảnh bitmap thì kỹ thuật giấu tin thường được sử dụng là các phương pháp biến đổi miền không gian của ảnh. Đối với ảnh nén thường sử dụng kỹ thuật giấu trên các hệ số biến đổi như DCT, DWT, DFT. Một số kỹ thuật phát hiện giấu tin theo định dạng ảnh như sau:

- Thuật toán áp dụng cho ảnh giấu tin trên LSB của miền tần số DCT.
- Kỹ thuật phát hiện giấu tin bằng phương pháp ước lượng thông tin giấu trên miền LSB.
- Phát hiện giấu tin trên hệ số Wavelet sử dụng kỹ thuật IWH (Integer Wavelet Histogram)

c) Phân tích theo thống kê

Phương pháp phân tích theo thống kê là phương pháp sử dụng các lý thuyết thống kê và thống kê toán học sau khi đã xác định được nghi vấn đặc trưng. Phương pháp này thường đưa ra độ tin cậy cao hơn và đặc biệt là cho các ảnh dữ liệu lớn.

- Kỹ thuật phát hiện giấu tin dựa trên phân tích tỉ lệ xám: đây là phương pháp dựa vào đặc trưng và tính chất của ảnh.
- Kỹ thuật phát hiện giấu tin dựa trên phân tích độ lệch chuẩn.
- Kỹ thuật phát hiện giấu tin bằng thống kê χ^2 một bậc tự do.

Trên đây là một số phương pháp chính được áp dụng trong quá trình phát hiện ảnh có giấu thông tin. Đối với mỗi phương pháp và kỹ thuật đều có những ưu điểm và nhược điểm riêng. Trong thực tế để có thể phát hiện ra ảnh có chứa thông tin sẽ bao gồm nhiều bước và giai đoạn. Ở mỗi bước và giai đoạn sẽ sử dụng các kỹ thuật khác nhau để tiền xử lý hoặc để loại bỏ những sai sót nhằm mang lại hiệu quả tốt nhất và nhanh nhất cho việc phát hiện ảnh chứa thông tin. Để có thể hiểu rõ hơn về cách thức tiến hành cũng như quy trình để phát hiện giấu tin trong ảnh của những phương pháp trên có thể tham khảo ở các tài liệu [16].

2.4. Câu hỏi ôn tập

Câu 1. Hãy trình bày về khái niệm giấu tin trong ảnh? Hãy trình bày 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 bày ví dụ về quy trình tách tin sử dụng kỹ thuật DCT? Hãy lấy ví dụ minh họa?
- Câu 10. Hãy trình bày khái niệm về kỹ thuật phát hiện giấu tin trong ảnh? Hãy nêu tên 5 kỹ thuật phát hiện giấu tin trong ảnh?
- Câu 11. 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?

CHƯƠNG 3: GIẤU TIN TRONG ÂM THANH

Chương 3 trình bày một số kiến thức liên quan đến 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. Ngoài ra, chương 3 đề cập đến một số phương pháp, kỹ thuật phát hiện giấu tin trong âm thanh.

3.1. Giới thiệu về giấu tin trong âm thanh

Do môi trường âm thanh có nhiều điểm khác biệt so với các môi trường đa phương tiện khác nên các kỹ thuật giấu tin trong âm thanh cũng đòi hỏi những yêu cầu và các phép xử lý khác nhau. Chính vì vậy, trong phần giới thiệu về giấu tin trong âm thanh, bài giảng sẽ đi vào làm rõ một số vấn đề cần lưu ý trong quá trình xử lý và giấu tin trong âm thanh.

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

Trong phần 1.2 bài giảng đã trình bày khái niệm về giấu tin trong âm thanh. Các vật chứa trong các kỹ thuật giấu tin trong âm thanh là các file âm thanh được đặc trưng bởi tần số, bước sóng, chu kỳ và biên độ, vận tốc lan truyền (tốc độ âm thanh).

Đặc điểm của kỹ thuật giấu tin trong âm thanh là giấu thông tin vào các khe hở của âm thanh. Các khe hở ở đây chính là các thành phần như: tần số, biên độ, chu kỳ,... của âm thanh. Các kỹ thuật giấu tin trong âm thanh lợi dụng vào điểm yếu hệ thống thính giác con người (Human Auditory System – HAS). Giấu tin trong âm thanh là kỹ thuật giấu tin đòi hỏi nhiều yêu cầu về lượng tin giấu và chất lượng giấu bởi vì hệ thống thính giác của con người rất nhạy cảm. Chính vì vậy, với bất kỳ thay đổi nào mà làm ảnh hưởng đến chất lượng âm thanh đều có thể bị phát hiện và tìm ra nhanh chóng. Tùy theo từng ứng dụng của giấu tin trong âm thanh mà sẽ có những yêu cầu đối với các kỹ thuật, thuật toán hoặc phương pháp giấu tin khác nhau. Tuy nhiên, trong trường hợp tổng quát các kỹ thuật giấu tin trong âm thanh ngoài việc phải đảm bảo các tính chất của kỹ thuật giấu tin vẫn cần phải đảm bảo một số yêu cầu đối với môi trường âm thanh như: Thông tin được giấu phải tồn tại được khi trải qua các phép biến đổi hay các hình thức tấn công cố ý hay vô tình. Thông tin giấu cần được toàn vẹn dưới bất kỳ hình thức tác động nào lên vật chứa (đối với các kỹ thuật nhúng thủy vân số trong âm thanh)

Một số vấn đề cần lưu ý trong kỹ thuật giấu tin trong âm thanh:

-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. Với một giây phát ra âm thanh, trích lấy một số mẫu biên độ đưa vào dữ liệu, con số ấy gọi là

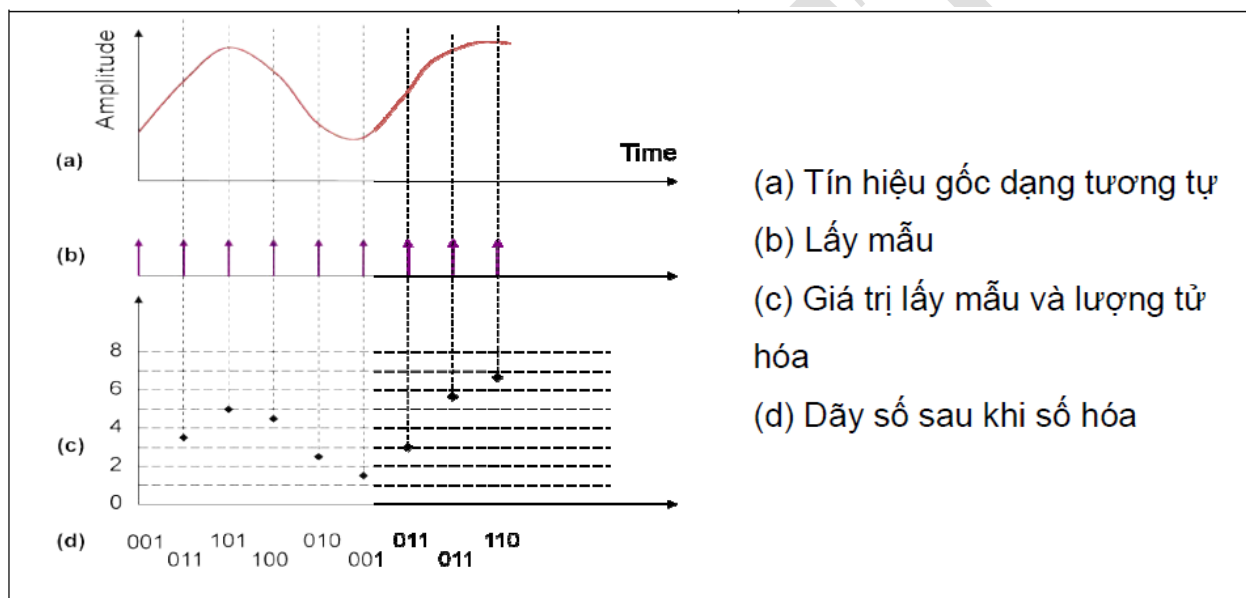
tần số trích mẫu (sample rate). Tần số này cho biết biên độ rung mỗi giây của sóng âm thanh. Thí dụ, tần số mẫu là 44,1 kHz thì mỗi giây tín hiệu nhận được bị cắt thành 44100 lát.

-Độ dày của bit: Để lưu lại dưới dạng số, mỗi mẫu được biểu diễn bằng một lượng bit dữ liệu nhất định nào đó, gọi là BitDepth. Với tập tin WAV thường là 8 hoặc 16 bits. BitDepth càng lớn thì âm thanh lấy mẫu càng chính xác và người nghe càng thấy sắc nét, trung thực. 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 tiêu tốn tới 10MB ổ cứng.

- Kích thước mẫu trích: Công thức kích thước mẫu trích (được tính bằng byte) như sau:

$$\text{LengthOfSample} = \text{Channels} * \text{AudioSampleSize} / 8.$$

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



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

3.1.2. Một số định dạng file âm thanh

Có thể phân loại định dạng file âm thanh thành một số định dạng chính như sau [15]:

- WAV (.wav): là kiểu định dạng đại diện cho âm thanh kỹ thuật số trong Windows PCs.
- 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.

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

Tên phần mềm giấu	Định dạng file âm thanh	Mã nguồn phần mềm
Info Stego	mp3	Trong hệ điều hành
ScramDisk	wav	Trong hệ điều hành
MP3Stego	mp3	Mã nguồn mở
StegoWav	wav	Mã nguồn mở
Hide4PGP	mp3, voc	Mã nguồn mở
Invisible Secrets	wav	Thương mại
Steganos	wav, voc	Thương mại

3.1.3. Phân loại một số phương pháp giấu tin trong âm thanh

Kỹ thuật giấu tin trong âm thanh đã và đang được ứng dụng nhiều trong thực tế hiện nay. Có nhiều phương pháp và kỹ thuật khác nhau đã được sử dụng để giấu thông tin vào âm thanh. Tiếp theo, bài giảng trình bày một số hướng để phân loại các kỹ thuật giấu tin trong âm thanh [1, 2].

a) 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 trong âm thanh. Theo tiêu chí này, các kỹ thuật giấu tin trong âm thanh chia làm một số kỹ thuật như sau:

- Kỹ thuật LSB;
- Kỹ thuật trải phổ;
- Kỹ thuật mã hóa pha;
- Kỹ thuật tiếng vang;
- Kỹ thuật tự đánh dấu.

b) Phân loại theo đặc điểm tín hiệu gốc

Đối với cách phân loại này, các chuyên gia 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. Trong một số trường hợp đặc biệt nhóm phương pháp này lại tỏ ra rất hiệu quả 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 bài giảng đã liệt kê về một số thuật toán và phương pháp, kỹ thuật giấu tin trong âm thanh khác nhau. Tiếp theo, để giúp người đọc hiểu hơn về thuật toán và kỹ thuật giấu tin trong âm thanh, bài giảng 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. Một số thuật toán khác không được mô tả trong bài giảng thì có thể tham khảo tại một số tài liệu [1, 2].

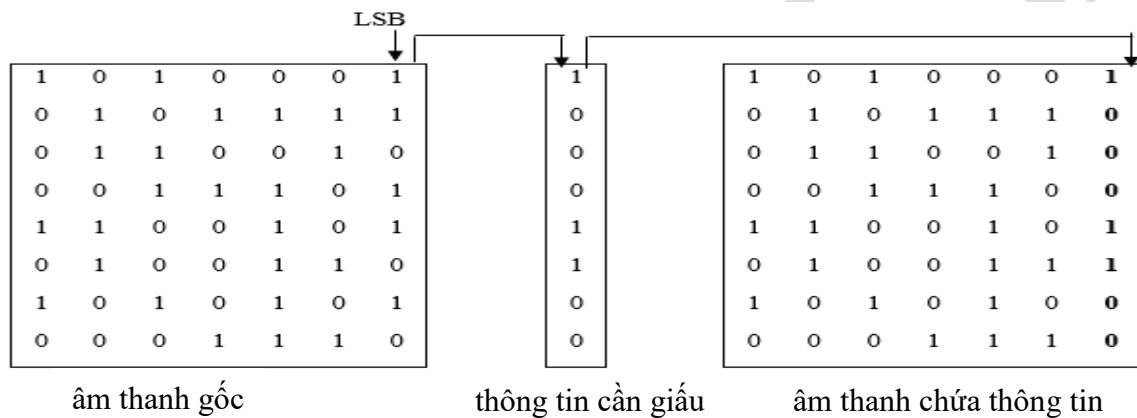
3.2. Phương pháp LSB

Cách thay thế LSB là cách đơn giản để nhúng thông tin vào một tệp âm thanh kỹ thuật số. Phương pháp LSB cho phép một lượng lớn dữ liệu được nhúng, tốc độ truyền dữ liệu nhanh. Chi tiết về phương pháp thay thế LSB đã được trình bày trong chương 2 (kỹ thuật giấu tin trong ảnh). Điểm cần lưu ý đối với phương pháp LSB trong âm thanh là thông tin sẽ được giấu vào trong file âm thanh. Để thực hiện được điều đó thì người giấu tin cần thực hiện những thao tác sau:

✓ Bước 1: Đọc file âm thanh gốc. Chia âm thanh gốc thành các segmen. Thông thường, người giấu tin sẽ chia file âm thanh các segmen dựa trên độ dài bit của thông tin cần giấu. Sau đó các segmen này được vector giá trị của tín hiệu, rồi lưu vào mảng một chiều để thực hiện giấu tin.

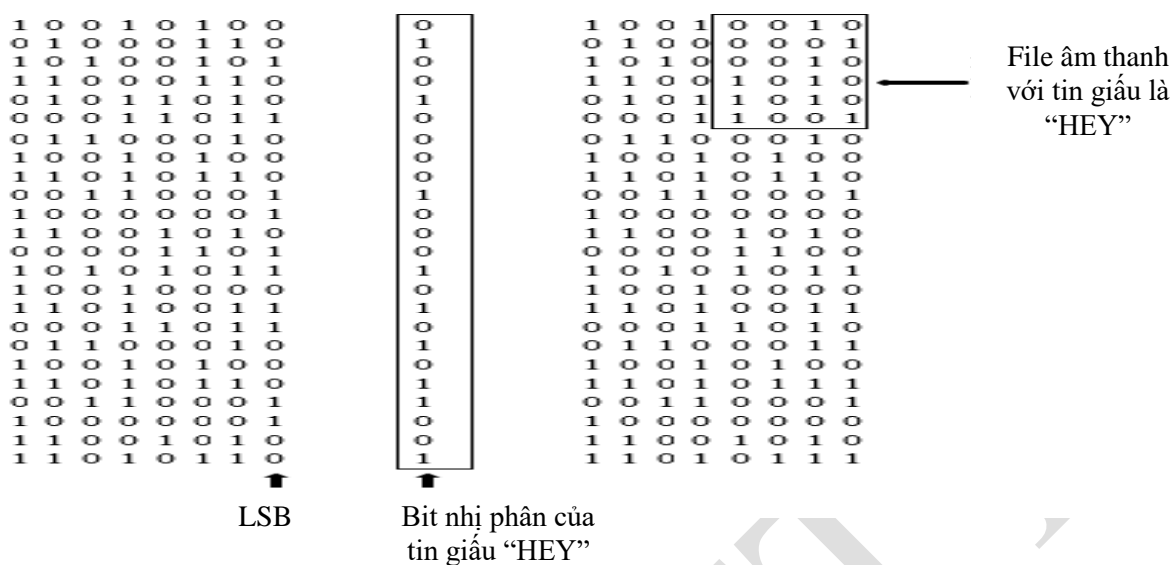
✓ Bước 2: Chuyển đổi thông tin cần giấu sang dạng nhị phân, tính độ dài bit của thông tin rồi lưu vào L .

- ✓ Bước 3: Chọn k là số bit LSB của tín hiệu âm thanh sẽ giấu sao cho phù hợp nhất.
- ✓ Bước 4: 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.
- ✓ Bước 5: Thực hiện giấu L bit đã tính vào các segmen. 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 chứ không phải 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 giải tin.
- ✓ Bước 6: Lưu lại tệp âm thanh kết quả F' được thông tin đã giấu.

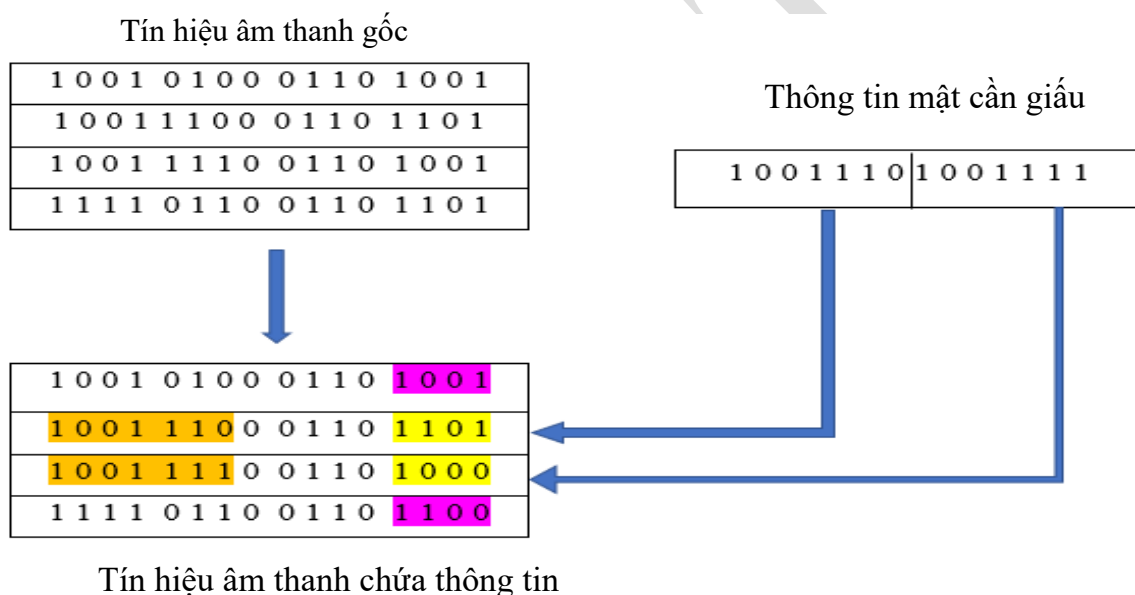


Hình 3.2. Mô tả phương pháp thay thế bit trong thuật toán LSB

Hình 3.2 thể hiện pháp thay thế LSB với trường hợp thay thế 1 bit LSB. Trong thực tế 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 bit 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 dưới đây 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 trong âm thanh hoạt động bằng cách thay pha của đoạn âm thanh ban đầu với pha được mã hóa của dữ liệu. Phương pháp mã hóa pha dựa vào tính chất là các thành phần của pha không gây ảnh hưởng đến hệ thống thính giác con người như nhiều. Như đã giới thiệu về HAS ở trên, HAS rất nhạy cảm trong miền thời gian nên dễ phát hiện ra thay đổi nhỏ. Nhưng Moore đã chứng minh được rằng HAS lại ít nhạy cảm với các thay đổi pha và đặc tính này được khai thác trong hệ thống nén âm thanh số [14, 18]. Ý tưởng của phương pháp này là

chia chuỗi âm thanh gốc thành các khối và nhúng toàn bộ dữ liệu vào phổ pha của khối đầu tiên (xem hình 3.5). Việc giấu tin sẽ được thực hiện bằng cách điều chỉnh pha trong phổ pha của dữ liệu [14].

3.3.2. Quy trình giấu tin bằng phương pháp mã hóa pha

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 $l(m)$. Lúc này áp dụng biến đổi Fourier có:

- Độ lớn tín hiệu được tính bằng công thức:

$$A_i(k) = \sqrt{\text{Re}[F\{c_i\}(k)]^2 + \text{Im}[F\{c_i\}(k)]^2}$$

- Ma trận độ lớn pha có các phần tử được tính theo công thức:

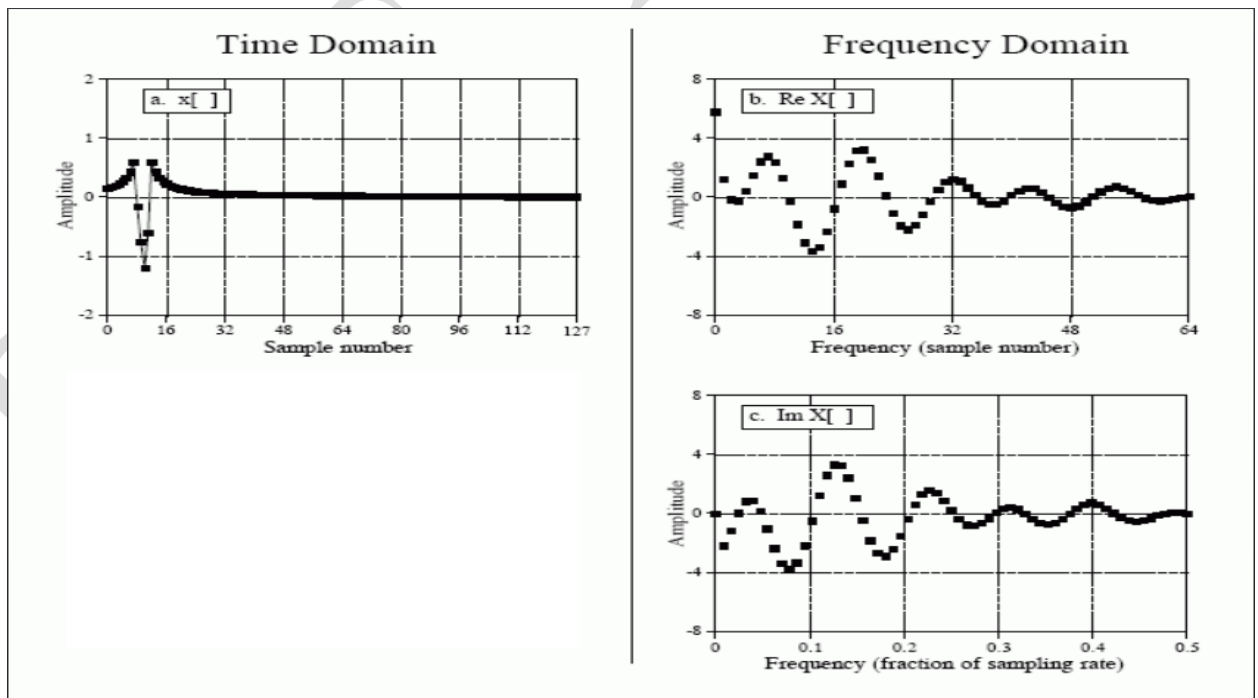
$$\varphi_i(k) = \arctan \frac{\text{Im}[F\{c_i\}(k)]}{\text{Re}[F\{c_i\}(k)]}$$

Trong đó:

R_e Là phần thực

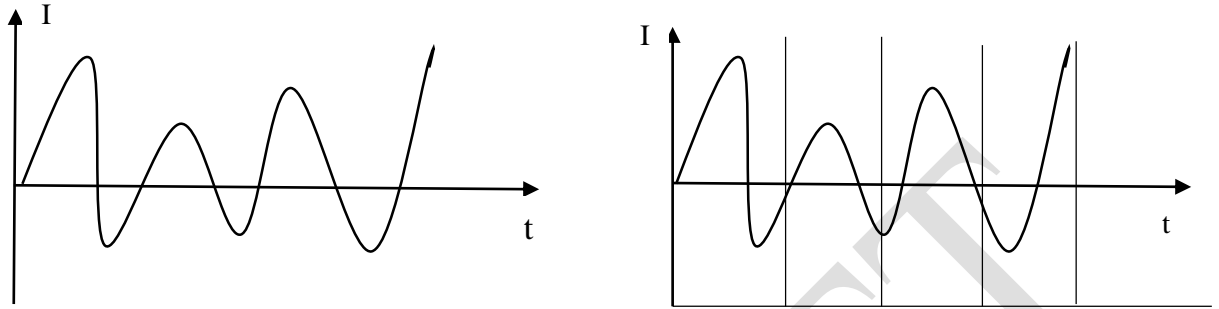
I_m Là phần ảo

t : là thời gian



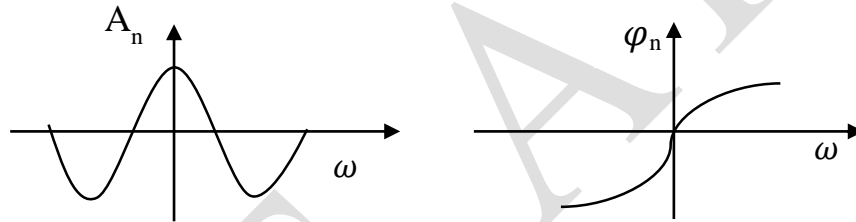
Hình 3.5. Phân tích các thành phần của dữ liệu âm thanh

Bước 1: Dữ liệu âm thanh gốc có chiều dài N được chia thành các segment có chiều dài bằng chiều dài với thông tin cần giấu.



Hình 3.5. Mô tả chia âm thanh gốc thành các segment bằng nhau

Bước 2: Mỗi đoạn segment 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 $0 \leq k \leq N/2 - 1$, $0 \leq j \leq N - 1$.



Hình 3.6. Minh họa khi mỗi đoạn được biến đổi bằng DFT

Bước 3: Tính độ lệch pha giữa các đoạn kề nhau bằng công thức sau:

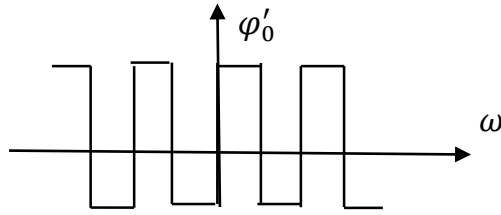
$$\Delta \varphi_j[\omega_k] = \varphi_{j+1}[\omega_k] - \varphi_j[\omega_k] \quad \forall j, k$$

Đây chính là quá trình tính sự khác biệt của ma trận pha với các ma trận xung quanh để tính ra mức độ chênh lệch. Việc tính toán này sẽ đảm bảo sự khác biệt giữa các pha sẽ không quá lớn sau khi tiến hành biến đổi.

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 segment liên tiếp phải được đảm bảo. Việc điều chỉnh pha của đoạn đầu được áp dụng dựa trên công thức:

$$\text{Phase_new} = \begin{cases} \frac{\pi}{2} & \text{nếu message bit} = 0 \\ -\frac{\pi}{2} & \text{nếu message bit} = 1 \end{cases}$$

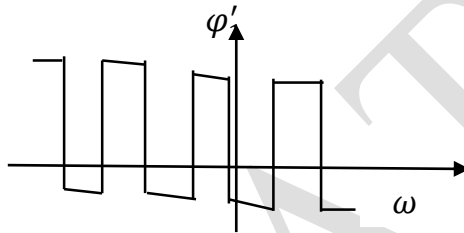
Khi đó thông tin giấu chỉ được phép giấu trong vector pha của đoạn đầu tiên.



Hình 3.7. 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:

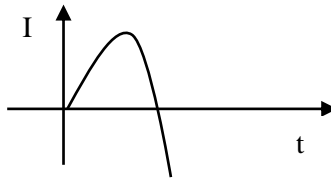
$$\varphi'_{j+1}[\omega_k] = \varphi'_j[\omega_k] + \Delta\varphi_{j+1}[\omega_k] \forall j, k$$



Hình 3.8. Ma trận pha mới được tạo

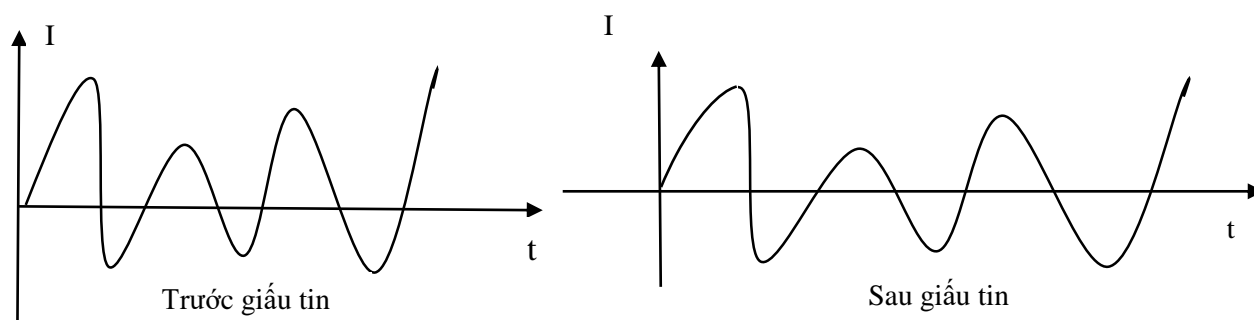
Trong thực tế luôn tìm được cặp $\varphi'_{j+1}[\omega_k]$ và $\varphi'_j[\omega_k]$ thỏa mãn công thức do Fourier rời rạc có tính đầy đủ (với mọi $N > 0$, mọi vector phức N chiều đều có một DFT và một IDFT đồng thời DFT và IDFT đều là các vector phức nhiều chiều). So sánh hình 3.7 và hình 3.8 thấy được là 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. Pha mới bằng pha kẻ trước đó cộng với độ lệch pha đã được tính ở trên



Hình 3.9. Pha mới được tạo ra sau khi kết hợp cường độ của pha cũ

Bước 7: Thực hiện ghép các segment 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 segment, sau đó thực hiện DFT để nhận tin.



Hình 3.10. So sánh pha trước và sau khi giấu tin

Từ hình 3.10 thấy được rằng: rõ ràng âm thanh đã bị thay đổi về cấu trúc pha khi giấu thông tin vào trong âm thanh.

3.3.3. *Đánh giá về phương pháp mã hóa pha*

a) Ưu điểm

- Như đã đề cập 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.
- Mã hóa pha không gây nhiễu như các phương pháp với LSB hoặc các phương pháp khác.

b) Nhược điểm

- Lượng thông tin được giấu nhỏ vì phương pháp mã hóa pha chỉ giấu được thông tin trên một đoạn nhỏ của file 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 file âm thanh, file đó có thể dễ dàng bị tấn công và phát hiện do thông tin mật chỉ ở đầu của file âm thanh.
- Thời gian nạp âm thanh tương đối lâu, trong khi chỉ có khối đầu tiên được nhúng thông tin, dữ liệu giấu không được phân bố đều trên toàn bộ tín hiệu âm thanh, sử dụng tài nguyên không hiệu quả.

3.4. Một số phương pháp khác

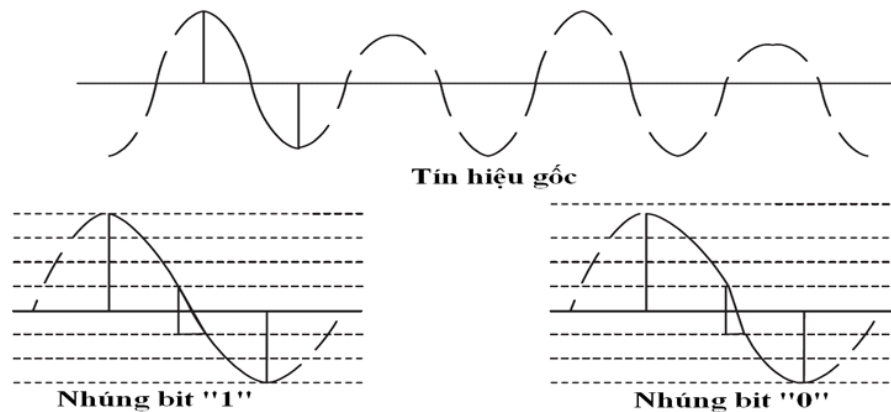
3.4.1. *Phương pháp tự đánh dấu*

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 dấu 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. Trong phương pháp bao gồm các kỹ thuật:

- Điều chỉnh tỉ lệ thời gian.
- Dựa và đặc trưng quan trọng nhất.

a) Điều chỉnh tỉ lệ thời gian

Phương pháp điều chỉnh tỉ lệ thời gian thực hiện bằng cách kéo dài hoặc rút ngắn tỉ lệ thời gian của 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 3.11 mô tả quy tắc giấu thông tin vào âm thanh dựa trên kỹ thuật điều chỉnh tỉ lệ thời gian.



Hình 3.11. Quy tắc giấu thông tin sử dụng phương pháp điều chỉnh tỉ lệ thời gian

Từ hình 3.11 thấy rằng: tín hiệu âm thanh khi chưa 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 tỉ lệ thời gian dẫn đến đường tín hiệu đi từ giá trị cực đại đến cực tiểu sẽ bị thay đổi độ dốc.

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:

Với dữ liệu đầu vào là:

- Tập âm thanh gốc C ;
- Chuỗi bit M cần giấu có độ dài L (L là bội số của 8).

Dữ liệu đầu ra là tập âm thanh chứa tin giấu C' .

- **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 $(L/4) * 7$.

- **Bước 2: Giấu tin**

Trong quá trình thực hiện giấu tin, kỹ thuật giấu tin bằng phương pháp điều chỉnh tỷ lệ thời gian thực hiện các tiến trình như sau:

✓ Đầu tiên là tiến trình kiểm tra dữ liệu: Đọc tệp chứa C , trích phần header và phần dữ liệu. Sau đó kiểm tra tệp chứa 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' .

✓ Tiếp theo là tiến trình thực hiện giấu: Trích tuần tự 3 mẫu dữ liệu của C và tính tổng:

- 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.

- 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.

- 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.

b) 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 của người nhúng và người rút trích. 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 như sau:

- Bước 1: Chia dữ liệu âm thanh thành các đoạn (frame) S_i có cùng kích thước n .
- 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 như sau:

$$S_i'(n) = \begin{cases} 0.99 * s_i(n) & \text{cho bit 1} \\ 0.98 * s_i(n) + 0.1 * s_i(n-d) & \text{cho bit 0} \end{cases}$$

Có thể thấy trong công thức trên nếu giá trị của $S_i(n)$ bằng với giá trị của $S_i(n-d)$ thì tổng $0.98 * S_i(n)$ và $0.1 * S_i(n-d)$ sẽ là $0.99 * S_i(n)$, tương ứng với trường hợp giấu bit 0. Mặc dù khả năng này ít xảy ra nhưng cũng có thể có dẫn đến khi rút trích tin sẽ lấy lại tin không đúng.

3.4.2. Phương pháp trải phổ

3.4.2.1. Khái niệm về phương pháp trải phổ

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 tối thiểu nhờ sử dụng mã giả ngẫu nhiên, mã này độc lập với tín hiệu thông tin. Bên nhận thông tin sẽ tiến hành giải trải bằng cách đồng bộ hóa mã giả ngẫu nhiên. 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. Các kỹ thuật trải phổ cố gắng trải thông tin mật vào trong phổ tần số của dữ liệu âm thanh càng nhiều càng tốt. Nó cũng tương tự như kỹ thuật LSB là trải ngẫu nhiên thông tin giấu trên toàn bộ file âm thanh. Như vậy, một hệ thống thông tin được coi là hệ thống trải phổ khi tín hiệu được phát có độ rộng băng tần lớn hơn nhiều so với độ rộng băng tần tối thiểu cần thiết và quá trình trải phổ được sử dụng bằng một mã giải độc lập.

Kỹ thuật trải phổ đang ngày càng được quan tâm và ứng dụng nhiều hiện nay. Ngoài những lợi ích về việc giấu tin an toàn thì các kỹ thuật trải phổ được ứng dụng rộng rãi là do:

- Giảm được khả năng dữ liệu sẽ bị hư hỏng hay bị làm cho nhiễu nhờ dùng các mã trải giả ngẫu nhiên làm cho nó khó bị nghe trộm.
- Đảm bảo độ an toàn truyền tin tránh bị các máy không có chủ đích thu và giải mã thông tin.
- Cho phép nhiều người dùng chung một giải băng tần nhờ đặc trưng tín hiệu tựa tạp âm.

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. Trong thực tế, các hệ thống giấu tin trong âm thanh sử dụng phương pháp trải phổ đã mang lại hiệu quả lớn và đặc biệt chúng rất an toàn trước các kỹ thuật tấn công.

3.4.2.2. Quy trình thực hiện trải phổ

Quy trình thực hiện trải phổ có thể hiểu một cách tổng quát như sau [18, 19, 20, 21, 22, 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 $\{s_1, s_2, \dots, s_n\}$. Trước khi đưa lên kênh truyền dẫn mỗi gói tin nhỏ s_i được trải phổ bằng một mã trải phổ giả nhiễu. Trong hệ thống trải phổ, mã giả ngẫu nhiên đóng một vai trò vô cùng quan trọng. Bởi vì nếu mã này là thực sự ngẫu nhiên thì ngay cả máy thu cũng không thể lấy lại được thông điệp vì chưa có phương pháp nào để đồng bộ với mã ngẫu nhiên thực sự. Chính vì vậy phải dùng mã giả ngẫu nhiên hay còn là mã mà máy thu mong muốn biết được còn đối với máy thu không mong muốn thì nó giống như tạp âm. 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 nén thông tin thì khi thu được những tín hiệu như vậy sẽ chỉ nhận biết được đây là nhiễu hoặc tạp âm.

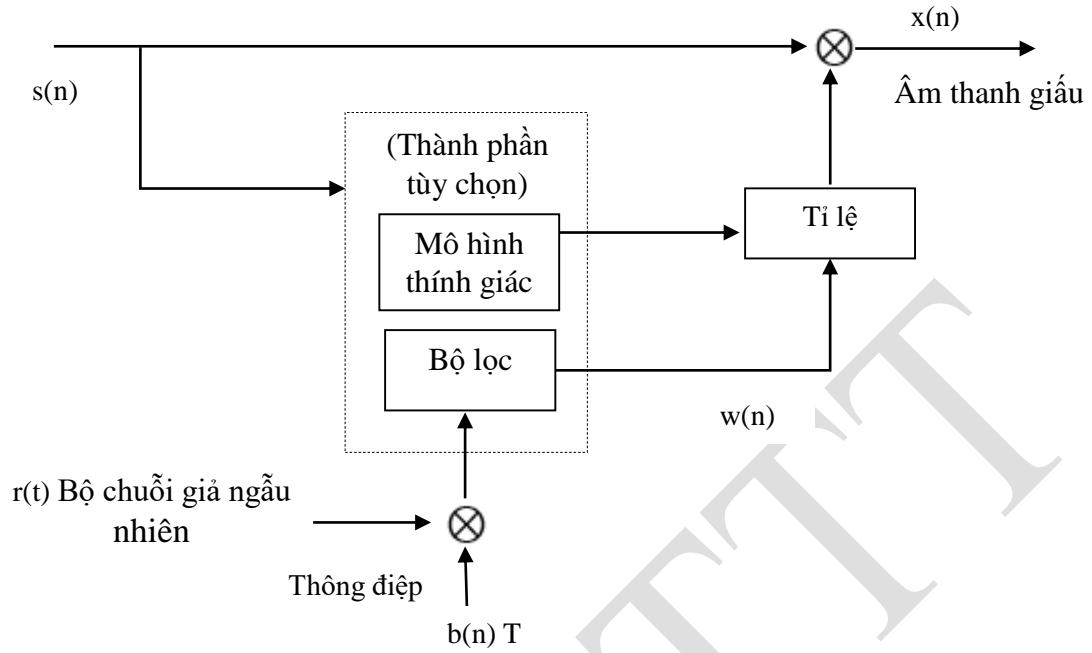
- Khi đến máy thu B , máy thu chủ định phải biết được bên phát là dùng mã nào để tạo ra một mã y hệt và đồng bộ mã để giải mã thông tin. Sau đó thực hiện nén phổ để thu được gói tin ban đầu. Các gói tin kết hợp với nhau sẽ thu được thông tin M .

3.4.2.3. Nhóm các phương pháp trải phổ

a) Phương pháp trải phổ truyền thống

Phương pháp trải phổ truyền thống là phương pháp dựa trên việc đồng bộ giữa tín hiệu âm thanh giấu và dãy chuỗi giả ngẫu nhiên. Các phương pháp trải phổ truyền thống đã được nghiên cứu và ứng dụng từ sớm. Trong một số nghiên cứu [21, 22, 23] đã trình bày cách thức giấu tin trong âm thanh bằng kỹ thuật trải phổ truyền thống. Ngoài ra, kỹ thuật trải phổ được áp dụng trong truyền thông, nên nếu dùng kỹ thuật trải phổ để giấu tin sẽ tận dụng được nguồn tài nguyên của thiết bị sẵn có. Ý tưởng của phương pháp trải phổ truyền thống được thể hiện như hình 3.12.

Trong mô hình chuỗi giả ngẫu nhiên được trải đều lên tín hiệu âm thanh. Các phép biến đổi được sử dụng như: DCT, DFT... 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 mật. Tín hiệu sau khi được điều chế $w(n) = br(n)$ 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. Tín hiệu sau khi điều chế $w(n)$ có giá trị bằng $r(n)$ hay không là phụ thuộc vào $v = 1$ hay $v = 0$. 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 $x(n) = s(n) + \alpha w(n)$



Hình 3.12. Ý tưởng trải phổ truyền thống

Phương pháp rò tìm thông điệp mật thường được sử dụng trong quá trình rút trích là tương quan tuyến tính. Hơn nữa, do chuỗi giả ngẫu nhiên $r(n)$ đã biết, có thể tạo dựng lại một khi biết khóa mật, thủy văn được dò tìm sử dụng phương pháp đồng bộ giữa $x(n)$ và $r(n)$. Công thức đồng bộ giữa $x(n)$ và $r(n)$ được mô tả như sau:

$$c = \frac{1}{N} \sum_{i=1}^N x(i) * r(i).$$

Trong đó, N là kích thước file âm thanh. Phương trình trên sinh tổng tương quan của hai thành phần sau:

$$c = \frac{1}{N} \sum_{i=1}^N x(i) * r(i) + \frac{1}{N} \sum_{i=1}^N \alpha b r^2(i)$$

Giả sử về thứ nhất của phương trình có biên độ nhỏ. Nếu hai thành phần tín hiệu $s(n)$ và $r(n)$ độc lập nhau, về thứ nhất sẽ bị triệt tiêu. Vì vậy, tín hiệu âm thanh gốc sẽ được tiên xử lý như hình để đạt được điều giả sử trên.

b) Phương pháp trải phổ cải tiến

Phương pháp trải phổ cải tiến đang được tiếp tục nghiên cứu, hoàn thiện và thu được các kết quả khác nhau. Theo tài liệu [19] các tác giả chia ra 3 hướng tiếp cận, ứng với các trường hợp: cực đại hóa tính bền vững, cực đại hệ số tương quan và hằng số bền vững. Tuy nhiên chưa có cách nào đề cập đến việc làm giảm xác suất bit lỗi khi rút trích thông tin. Sau

cùng, kỹ thuật trải phổ cải tiến [23] đã thực hiện chuyển tín hiệu gốc thành nguồn giao thoa, làm tăng tính bền vững của quá trình trích rút thông tin một cách đáng kể. Ý tưởng của phương pháp [23] là sử dụng lại kiến thức của bộ mã hóa về tín hiệu đó (hay chính là việc dùng hình chiếu của dãy tín hiệu trên tín hiệu giả). So với phương pháp truyền thống thì trải phổ cải tiến đã có sự biến đổi:

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

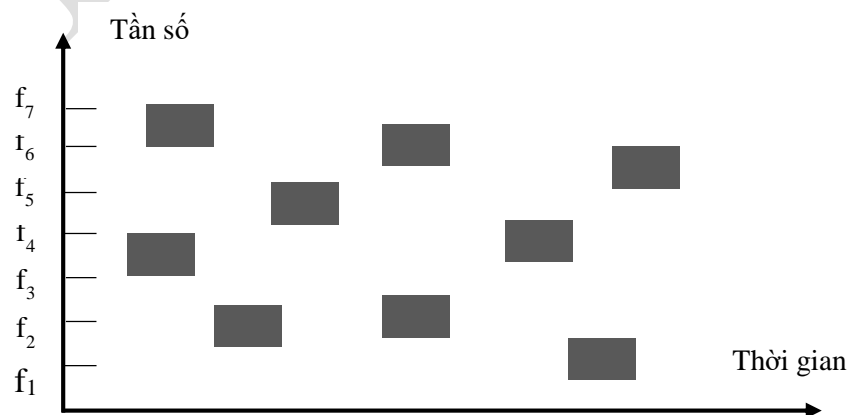
Trong đó $\mu(cx, b)u$ là hàm nhúng của $cx = \frac{\langle x, u \rangle}{\|u\|}$. Dễ nhận thấy trải phổ truyền thống là một trường hợp đặc biệt của phương pháp trải phổ cải tiến.

3.4.2.4. 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, nhảy tần, nhảy thời gian và hệ lai. Nhưng hai phương pháp trải phổ sử dụng trong việc giấu tin trong âm thanh là DSSS (Direct Sequence Spread Spectrum) và FHSS (Frequency Hopped Spread Spectrum). Tiếp theo, bài giảng sẽ trình bày chi tiết về cách thức tiến hành giấu tin trong âm thanh sử dụng các phương pháp DSSS và FHSS.

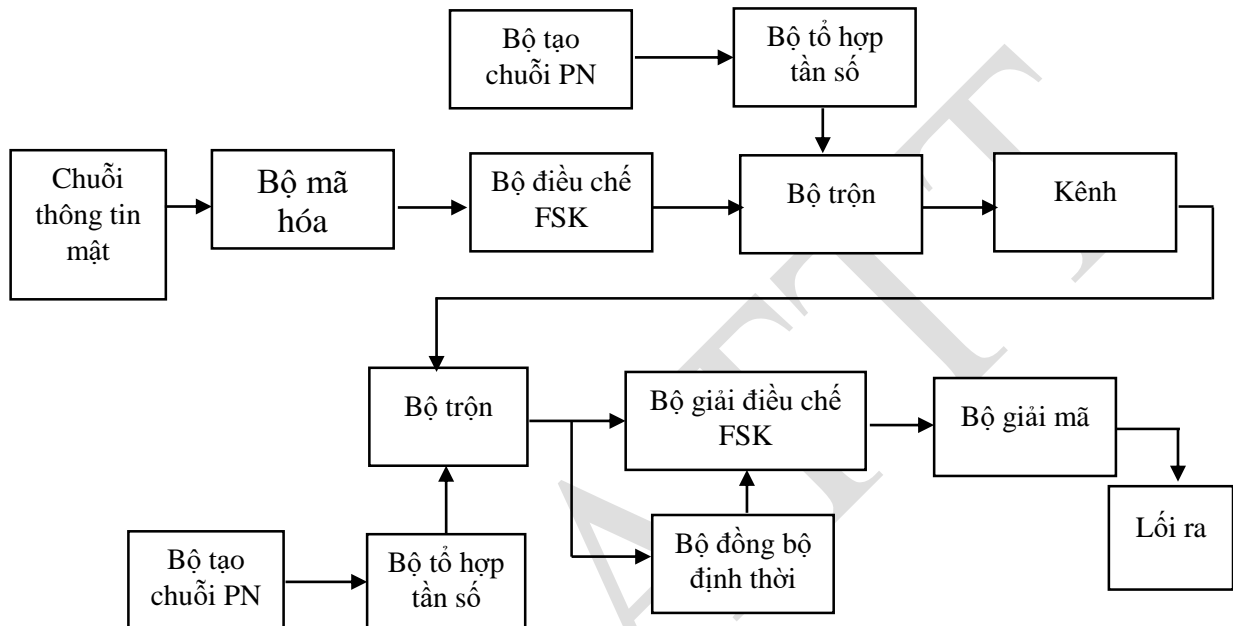
a) Phương pháp trải phổ nhảy tần (Frequency Hopping Spread Spectrum- FHSS)

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 kênh 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 lỗi ra của một bộ tạo chuỗi giả ngẫu nhiên. Hình 3.13 mô tả về quy trình trải phổ nhảy tần.



Hình 3.13. Minh họa về trải phổ nhảy tần

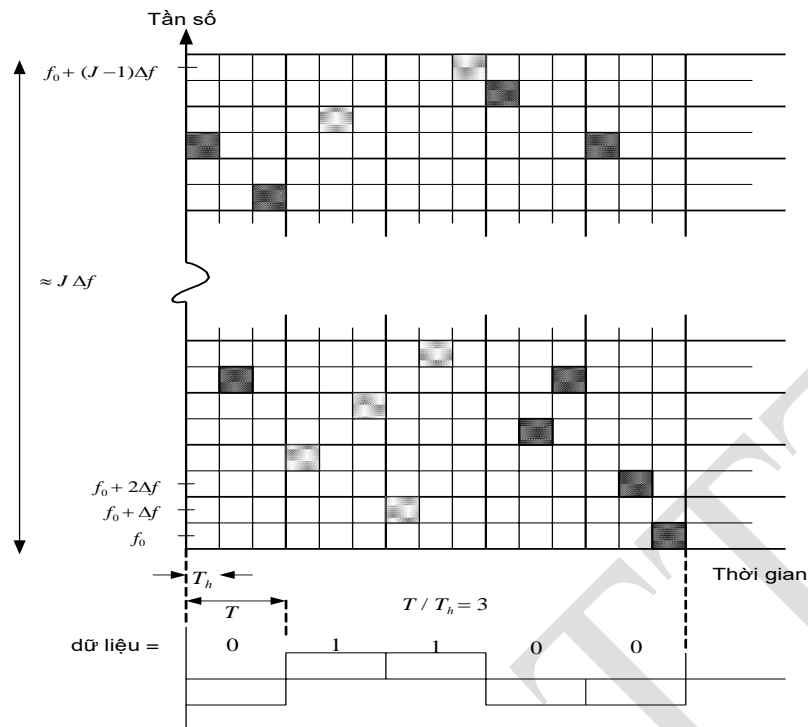
Dựa trên tốc độ nhảy của tần số thì phương pháp trải phổ nhảy tần được chia làm 2 loại đó là trải phổ nhảy tần nhanh (khi tốc độ nhảy nhanh hơn tốc độ dữ liệu) và trải phổ nhảy tần chậm (khi tốc độ nhảy chậm hơn tốc độ dữ liệu). Nhìn chung thì cả hai phương pháp này chỉ khác nhau về tốc độ nhảy, còn nguyên lý hoạt động của hai phương pháp tương tự nhau. Hình 3.14 mô tả về nguyên lý hoạt động của trải phổ nhảy tần.



Hình 3.14. Sơ đồ khối của hệ thống trải phổ FHSS

Chi tiết quy trình trải phổ của hệ thống trải phổ FHSS như sau:

- Ở phía máy phát: tín hiệu đầu vào của hệ thống trải phổ nhảy tần bao gồm:
 - ✓ Chuỗi thông tin mật cần được truyền đi: Chuỗi thông tin này 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. Ở một số loại máy phát đời đầu thì không có bộ mã hóa này. Bước này có nhiệm vụ làm tăng tính bảo mật của thông tin trên đường truyền. Phương pháp giải mã và khóa bí mật sẽ được người gửi và người nhận thỏa thuận bằng một hình thức nào đó. Tín hiệu sau khi được mã hóa sẽ được đưa vào bộ điều chế FSK (điều chế số theo tần số tín hiệu). Tại đây, tín hiệu đã mã hóa sẽ được bộ FSK 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.



Hình 3.15. Biểu đồ tần số của tần nhanh với FSK

Ví dụ: Trên hình 3.15 là biểu đồ tần số của nhảy tần nhanh với FSK. Trong đó 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 và 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 cho chất lượng tín hiệu tốt hơn (xác suất lỗi bit ít hơn so với tập không trực giao). 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 tô nhạ khi bit dữ liệu là 1 hoặc bởi ô tô đậm khi bit 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.

✓ Bộ tạo chuỗi PN: 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 số thì bộ tạo chuỗi giả ngẫu nhiên này tạo ra một đoạn chứa m bit của mã để điều khiển bộ tổng hợp tần số để tạo ra các giá trị tần số nhảy tần cho sóng mang. Ở đây, chuỗi giả ngẫu nhiên không nhất thiết phải là dãy nhị phân. Khác với hệ thống trải phổ trực tiếp, chuỗi giả ngẫu nhiên ở hệ thống trải phổ nhảy tần chỉ dùng để điều khiển hoặc xác định các mẫu nhảy. 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 PN, 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 PN.

Như vậy hai dữ liệu đầu vào là thông tin mật và chuỗi giả ngẫu nhiên được qua các hàm và các phép tiền xử lý thì thu được $x(t)$ và $y(t)$. 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 sau khi qua Bộ trộn sẽ được phát qua kênh truyền dẫn, kênh này có thể là kênh dưới đất hoặc kênh vệ tinh. Tín hiệu khi được đưa lên kênh có thể gây ra giảm chất lượng như: nhiễu, tạp âm, suy hao công suất tín hiệu.

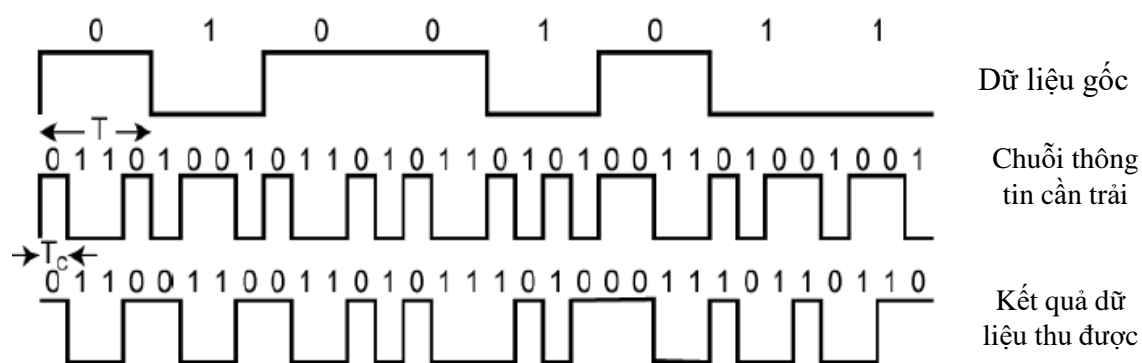
- Ở phía máy thu: tín hiệu từ kênh truyền sau khi thu về sẽ được đưa vào bộ trộn. Nhận được tín hiệu truyền về, bộ tạo chuỗi PN sẽ tạo nên chuỗi giả ngẫu nhiên đồng bộ với chuỗi tới (Bộ tạo chuỗi giả ngẫu nhiên ở phía máy phát và máy thu là như nhau và được đồng bộ với nhau giao tiếp với bộ tổ hợp tần số ở phía phát và phía thu.). 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 lõi 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 lõi 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. Tín hiệu sau khi được đưa qua bộ trộn thì được đồng bộ về mặt thời gian tại Bộ đồng bộ định thời. Kết quả tín hiệu sau khi được đồng bộ thời gian được gửi cho bộ giải điều chế FSK. Tại đây, tín hiệu sóng mang $x(t)$ được đưa vào bộ giải điều chế FSK để tái tạo lại dữ liệu trước khi bị mang đi điều chế. Dữ liệu sau khi được giải điều chế được đưa vào bộ giải mã để giải mã, khôi phục lại dữ liệu gốc ban đầu.

Nhận xét: Tính hiệu quả của phương pháp trải phổ nhảy tần chính là bên nhận và bên gửi sẽ phải thống nhất với nhau chuỗi giả ngẫu nhiên để thu được thông tin một cách chính xác.

b) Phương pháp trải phổ dãy trực tiếp (Direct Sequence Spread Spectrum - DSSS)

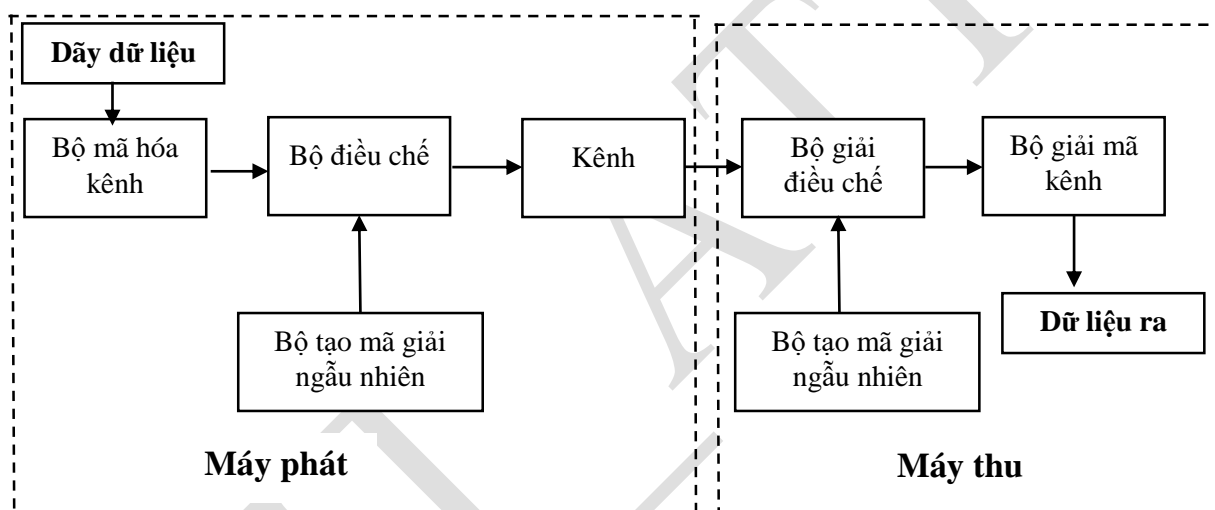
➤ Khái niệm

DSSS là hệ thống trải phổ dãy trực tiếp, rất phổ biến và được sử dụng rộng rãi trong các công nghệ trải phổ vì nó dễ dàng cài đặt và có tốc độ cao. DSSS là một phương pháp truyền dữ liệu trong đó hệ thống truyền và hệ thống nhận đều sử dụng một tập các tần số có độ rộng 22 MHz. Các kênh rộng này cho phép các thiết bị truyền thông tin với tốc độ cao hơn hệ thống FHSS nhiều.



Hình 3.16. Minh họa trải phổ dây trực tiếp

➤ Nguyên lý hoạt động



Hình 3.17. Sơ đồ khối hệ thống trải phổ DSSS

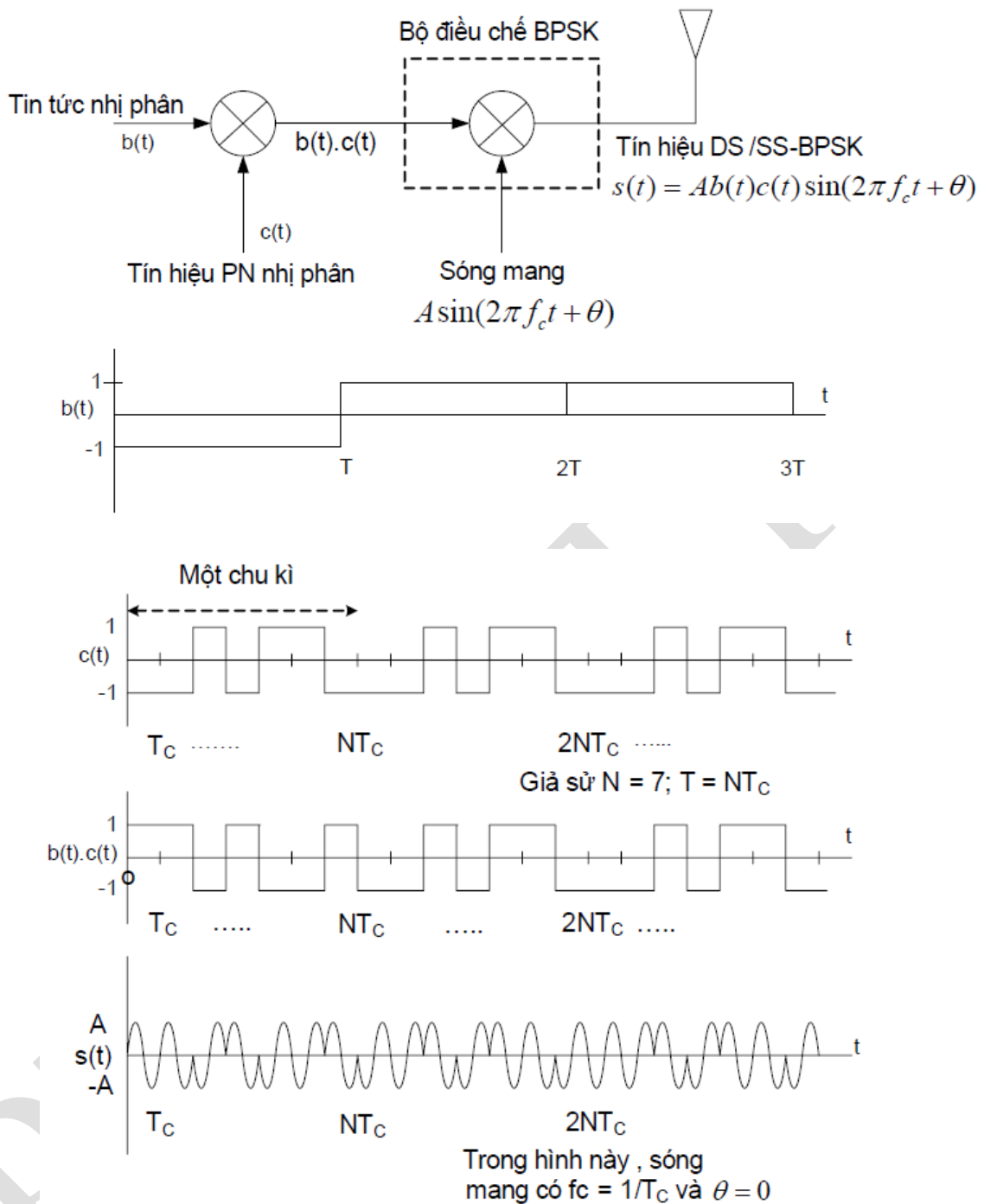
Các phần tử cơ sở của hệ thống trải phổ DSSS được minh họa trên hình 3.17. Từ hình 3.17 thấy được quy trình trải phổ của hệ thống trải phổ DSSS như sau:

- Ở phía máy phát: tín hiệu đầu vào của hệ thống trải phổ trực tiếp là:
 - ✓ Dữ liệu dạng nhị phân (tín hiệu cần trải phổ). Tín hiệu này được đưa vào Bộ mã hóa kênh (còn gọi là bộ lập mã hiệu chỉnh lỗi hay bộ mã hóa sửa sai). Tại đây, tín hiệu đầu vào 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.
 - ✓ Bộ tạo mã giả ngẫu nhiên tạo ra một chuỗi giả ngẫu nhiên dạng nhị phân, chuỗi này được đưa vào bộ điều chế để trải tín hiệu được phát đi về phổ. Trên thực tế, hai bộ tạo mã

giả ngẫu nhiên từ bên phía máy phát và máy thu phải như nhau và được đồng bộ với nhau giao tiếp với bộ điều chế và giải 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 trao 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 nhân hai tín hiệu này với nhau. Quá trình nhân hai tín hiệu với nhau thực chất là quá trình trải phổ. Kết quả là phổ của tín hiệu nhận được 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 được gán theo phương pháp BPSK hoặc QPSK (đây là quá trình điều chế sóng mang theo phương pháp BPSK hoặc QPSK). Kết quả là tín hiệu trải phổ sau khi được điều chế sóng mang thì được đưa lên kênh truyền dẫn. Hình 3.18 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. Kênh này có thể gây ra giảm chất lượng như: nhiễu, tạp âm, suy hao công suất tín hiệu.



Hình 3.18. Bộ điều chế BPSK

- Ở phía máy thu: tín hiệu sau khi được lấy trên kênh truyền dẫn về sẽ được đưa vào bộ giải điều chế. Nhận được tín hiệu truyền về, bộ tạo mã giả 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 giải điều chế để 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.

Như vậy, tại đầu thu, máy thu cố gắng khôi phục lại tín hiệu gốc bằng cách khử các quá trình sử dụng ở máy phát. Chú ý rằng bộ nén/giải nén dữ liệu và bộ mã sửa sai/ giải mã là tùy chọn. Chúng dùng để cải thiện chất lượng hệ thống.

Nhận xét: Với việc giấu thông tin mật áp dụng phương pháp trải phổ DSSS thì trải tín hiệu mật ra bằng một hằng số gọi tốc độ chip. Đồng thời điều chỉnh độ dài tối đa của tín hiệu giả ngẫu nhiên và thêm vào phương tiện chứa. Phổ của thông tin mật được trải rộng làm cho chuỗi thông tin mật giảm dần và được thêm vào phương tiện chứa như là thêm nhiều ngẫu nhiên. Quá trình thu nhận phổ để tách thông tin thì người nhận cần phải biết điểm bắt đầu và kết thúc của dữ liệu được trải phổ, tốc độ chip, tốc độ dữ liệu.

Kết luận: Mỗi hệ thống trải phổ có những ưu và nhược điểm riêng. Và việc lựa chọn hệ thống nào để sử dụng còn phụ thuộc vào ứng dụng cụ thể. Nếu như DSSS làm giảm công suất nhiễu bằng cách trải nó trên phổ tần rộng thì FHSS tại thời điểm bất kì đã cho người dùng khác nhau phát các tần số khác nhau vì thế tránh được nhiễu. 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 – PCN), WLAN (Wireless Local Area Networks), Tổng đài nhánh cá nhân vô tuyến (Wireless Private Branch Exchanges – WPBX), 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 - GPS). Các công nghệ ứng dụng kỹ thuật trải phổ cung cấp các khả năng:

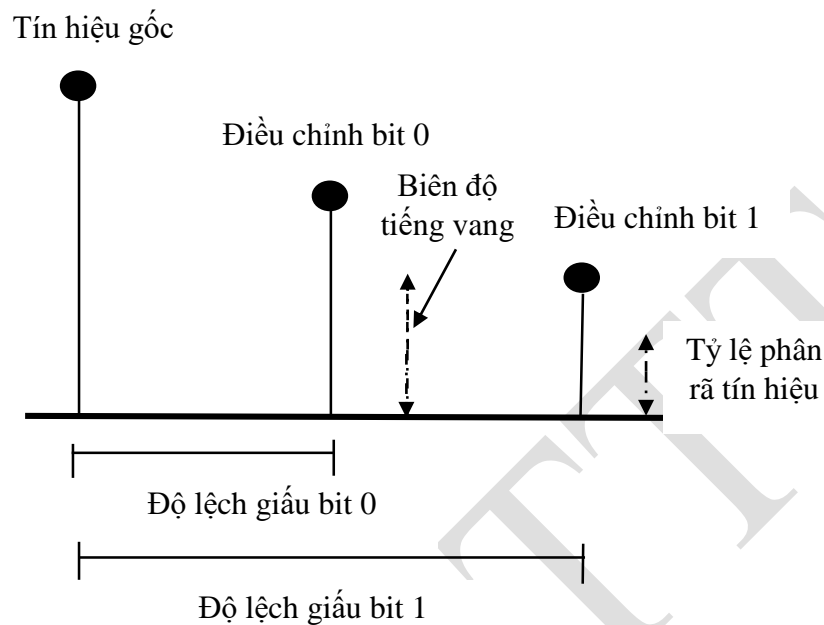
- Khả năng chống lại nhiễu cố ý và không cố ý – đặc điểm quan trọng đối với thông tin trong các vùng đông đúc như thành phố;
- Có khả năng loại bỏ hoặc giảm nhẹ ảnh hưởng của truyền lan đa đường, có thể là vật cản lớn trong thông tin thành phố;
- Có thể chia sẻ cùng băng tần với các người dùng khác nhờ tính chất tín hiệu giống như tạp âm của nó;
- Có thể dùng cho thông tin vệ tinh đã cấp phép trong chế độ CDMA; Cho mức độ riêng tư nhất định nhờ dùng các mã trải giả ngẫu nhiên làm cho nó khó bị nghe trộm.

3.4.3. Phương pháp Echo

a) Định nghĩa

Kỹ thuật giấu tin bằng phương pháp Echo (tiếng vang) được thực hiện bằng cách thêm tiếng vang vào trong tín hiệu gốc. Dữ liệu nhúng sẽ thay đổi 3 tham số của tiếng vang là biên độ ban đầu, tỉ lệ phân rã và độ trễ. 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. Ngoài ra, số lượng tin giấu còn liên quan đến thời gian trễ của tiếng vang và biên độ của nó.



Hình 3.19. Các tham số chính trong phương pháp mã hóa tiếng vang

Các tham số chính trong quy trình giấu thông tin trong âm thanh bằng phương pháp mã hóa tiếng vang gồm (xem hình 3.19):

- 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 $c(t)$:

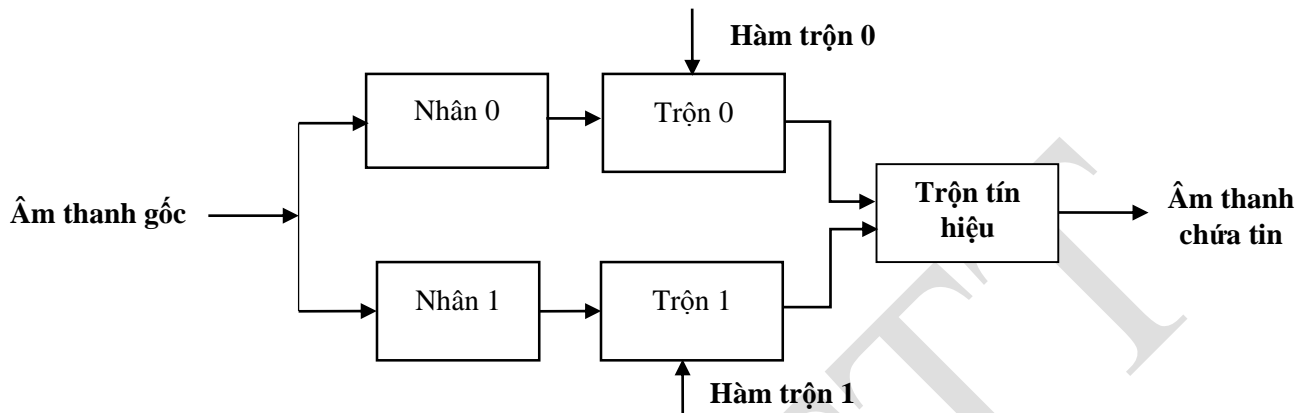
$$c(t) = f(t) + \alpha f(t - \Delta t)$$

Thông tin được mã hóa thành các tín hiệu bằng cách hiệu chỉnh khoảng thời gian Δt . Δt là khoảng thời gian dừng giữa tín hiệu phát và tiếng vang. Tại bước mã hóa, người gửi có thể chọn các giá trị Δt và $\Delta t'$ tương ứng với các bit 0 hoặc 1 được nhúng. Các giá trị này được chọn sao cho tín hiệu tiếng vang không gây ra bất kỳ sự nghi ngờ nào tới cho người nghe.

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

b) Quy trình giấu tin



Hình 3.20. Sơ đồ tổng quát phương pháp mã hóa tiếng vang

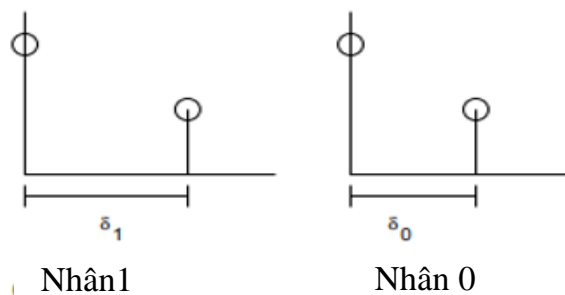
Từ sơ đồ tổng quát cho thấy các tham số chính trong quy trình giấu tin sử dụng phương pháp mã hóa tiếng vang gồm:

- Tín hiệu ban đầu
- Nhân hệ thống mã hóa
- Tín hiệu trộn

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 mã hóa tiếng vang như sau:

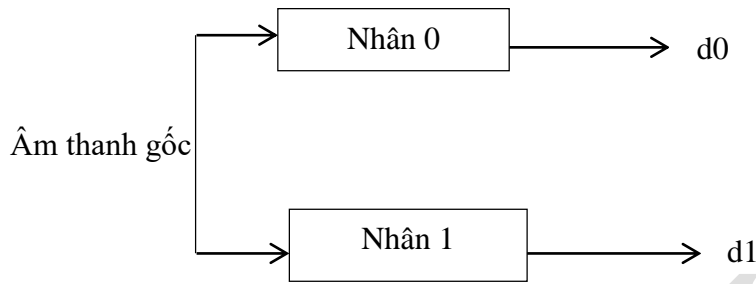
Bước 1: Tín hiệu ban đầu là tệp âm thanh gốc có dạng là hàm rời rạc theo thời gian $F(t)$. Tín hiệu ban đầu được xác định dựa vào hàm $F(t)$, từ tín hiệu ban đầu này để tìm ra được tiếng vang.

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 3.21. 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 3.22. Đầu vào và đầu ra bước 2

Kết quả thu được là hai đường tiếng vang $d0$ và $d1$ có dạng:

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

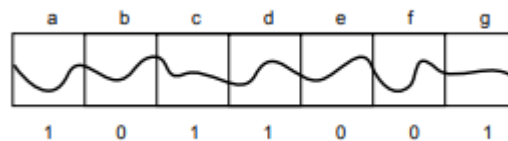
trong đó:

$F(t)$ là hàm rời rạc theo thời gian

β là tỷ lệ phân rã

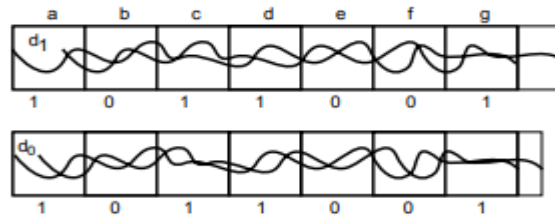
Δt là độ trễ của echo so với âm thanh gốc

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 $N \cdot L$ không lớn hơn độ dài của tín hiệu âm thanh. Mỗi phần có thể được lặp lại với các bit mong muốn bằng cách xem xét mỗi phần như một tín hiệu độc lập. Âm thanh sau khi được giấu tin sẽ là tái kết hợp của tất cả các tín hiệu mã hóa độc lập. Để nối hai đoạn mã hóa khác nhau sử dụng tín hiệu trộn 0 hoặc 1. Ví dụ: tín hiệu được chia thành 7 phần a, b, c, d, e, f, g.



Hình 3.23. Ví dụ giấu bit 0 và bit 1

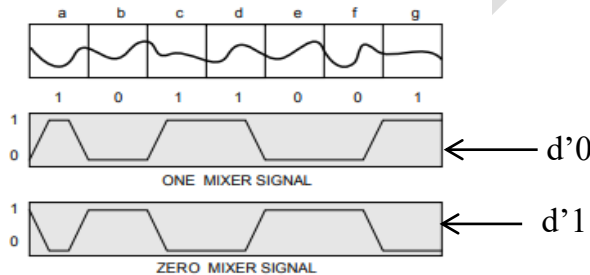
Thấy rằng: Các phần a, c, d, g chứa các bit 1 phần còn lại chứa bits 0. Theo lý thuyết kỹ thuật mã hóa tiếng vang sẽ mã hóa từng phần và sử dụng từng loại nhân phù hợp với bit cần giấu nhưng trong thực tế các chuyên gia đã mã hóa toàn bộ sử dụng nhân 0 hoặc nhân 1, nên kết quả sẽ thu được hai tiếng vang đó là $d0$ và $d1$.



Hình 3.24. Kết quả tiếng vang sử dụng nhân 0 và nhân 1

Bước 3: 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 khi tín hiệu muốn chuyển đổi được đưa vào. 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.



Hình 3.25. Kết quả của hàm trộn

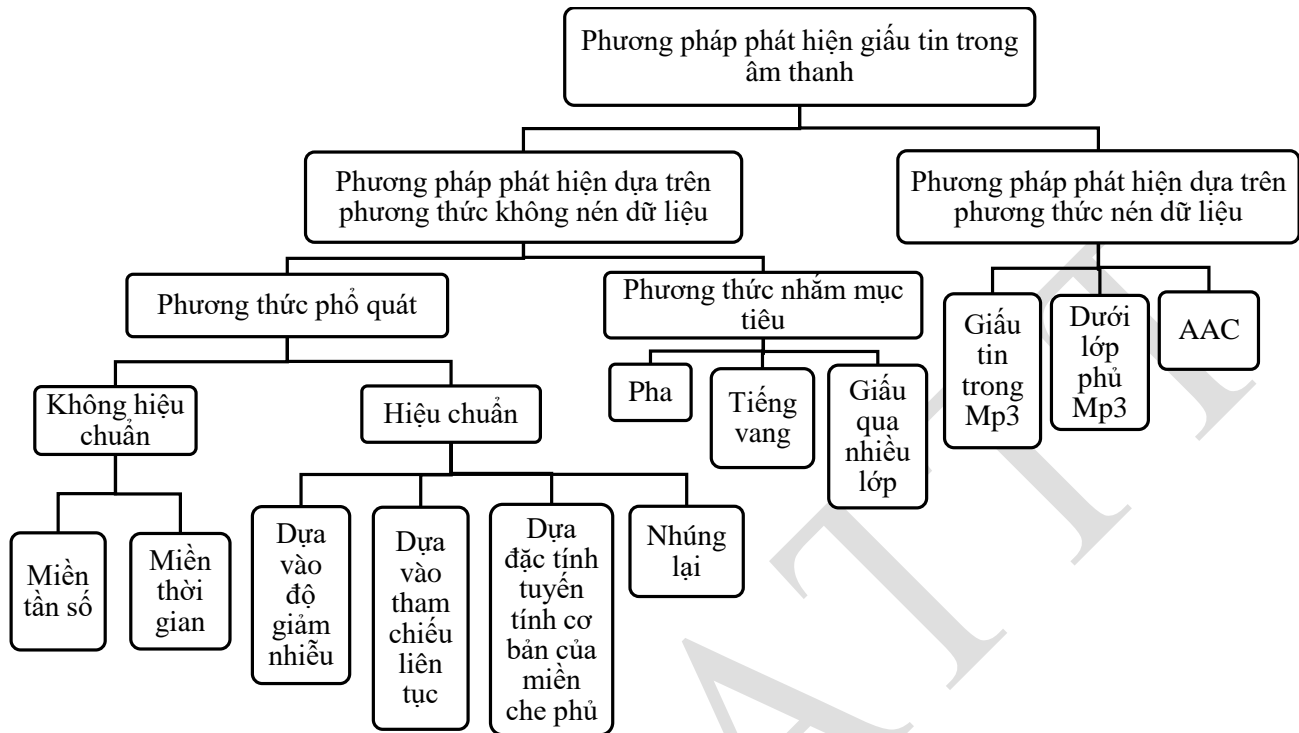
Bước 4: Kết hợp 2 tín hiệu trộn thu được tín hiệu mã hóa khi cộng 2 tín hiệu, những đoạn có giá trị bằng 1 là mã hóa bit 1, đoạn có giá trị 0 là mã hóa bit 0, những đoạn có giá trị nằm trong khoảng từ 0 đến 1 là đoạn chuyển tiếp giữa 2 đoạn mã hóa khác nhau (giữa 2 đoạn mã hóa khác nhau 0 và 1).

Lưu ý: Tổng giá trị của hai tín hiệu trộn luôn bằng 1, hai tín hiệu trộn này cộng lại với nhau bằng 1 nên có độ mịn chuyển đổi giữa các phần được mã hóa khác nhau và ngăn chặn thay đổi đột ngột trong cộng hưởng của tín hiệu cuối cùng.

3.5. Phương pháp phát hiện giấu tin trong âm thanh

Phương pháp phát hiện giấu tin trong âm thanh là kỹ thuật phát hiện sự tồn tại của thông tin ẩn giấu trong âm thanh. Mục đích của các phương pháp phát hiện giấu tin trong âm thanh là phát hiện ra âm thanh có mang thông tin và tìm cách lấy ra thông tin mật đó hoặc làm mất tính toàn vẹn của thông tin đó. Có nhiều phương pháp và kỹ thuật khác nhau để có thể

phát hiện ra âm thanh có giấu tin [32]. Hình 3.26 liệt kê một số phương pháp cơ bản để phát hiện âm thanh có giấu tin đang được biết đến hiện nay.



Hình 3.26. Phân loại các kỹ thuật phát hiện giấu tin trong âm thanh

Từ sơ đồ phân loại các kỹ thuật phát hiện giấu tin trong âm thanh có thể thấy rằng: trong lĩnh vực phát hiện giấu tin trong âm thanh hiện nay đang có hai hướng chính [32]:

a) Phát hiện dựa vào các file âm thanh nén:

Phát hiện dựa vào các file âm thanh nén là phương pháp mà khi kẻ tấn công thu được file âm thanh chúng sẽ dựa vào đặc tả của file âm thanh để xây dựng phương pháp phát hiện.

b) Phát hiện dựa vào các file âm thanh không nén:

Kỹ thuật phát hiện dựa vào các file âm thanh không nén sẽ có những phương pháp khác nhau để phát hiện như: phát hiện khi biết được phương pháp giấu tin hoặc phát hiện khi chưa biết phương pháp giấu tin.

3.6. Câu hỏi ôn tập

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 dải trực tiếp?
- Câu 11. Hãy trình bày về phương pháp mã hóa tiếng vang?
- Câu 12. Hãy trình bày về một số phương pháp phát hiện giấu tin trong âm thanh?
- Câu 13. Hãy trình bày về 3 ứng dụng của giấu tin trong âm thanh trong thực tế?

CHƯƠNG 4: GIẤU TIN TRONG VIDEO

Chương này trình bày một số kiến thức liên quan đến kỹ thuật giấu tin và tách tin trong video. Bên cạnh đó, trong chương này bài giảng đề cập đến một số phương pháp phát hiện tin giấu trong video...

4.1. Giới thiệu về phương pháp giấu tin trong video

4.1.1. Đặc điểm của giấu tin trong video

Các file video được được đặc trưng các khung hình và khung âm thanh. Mỗi khung hình là một ảnh kỹ thuật số trực giao bitmap bao gồm một raster các điểm ảnh (pixel). Pixels chỉ có một thuộc tính màu sắc của chúng. Màu sắc của một điểm ảnh được biểu diễn bởi một giá trị cố định các bit.

Kỹ thuật giấu tin trong video trước kia chỉ tập trung vào việc giấu tin vào các khung hình của file video do các kỹ thuật này thường mang lại hiệu quả cao. Tuy nhiên, trong một thời gian gần đây kỹ thuật giấu tin trong khung âm thanh của video cũng đang được nghiên cứu và áp dụng nhiều trong thực tế. Bên cạnh đó, do đặc tính của file video là tập hợp các khung hình và âm thanh nên trong quá trình thực hiện giấu tin trong video cần phải lưu ý đến một số tham số đặc trưng của video. Các tham số gồm: Pixel mỗi khung hình, Bit trên mỗi khung hình; kích thước video... Để làm rõ hơn về các tham số này, 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 (R x C) ở độ sâu màu 24 bit và tỷ lệ khung hình 25 fps (số khung hình được hiển thị trong 1s). Các đặc trưng của một số tham số được tính như sau [10, 14, 24]:

- Pixel mỗi khung hình = $640 * 480 = 307.200$
- Bit trên mỗi khung hình = $307.200 * 24 = 7.372.800 = 7,37 \text{ Mbits}$
- Tỷ lệ bit (BR) = $7.37 * 25 = 184,25 \text{ Mbits / sec}$
- Kích thước video (VS) = $184 \text{ Mbits / sec} * 3600 \text{ giây} = 662.400 \text{ Mbits} = 82.800 \text{ MB}$

4.1.2. Một số định dạng file video

Cũng giống như các kỹ thuật giấu tin trong môi trường đa phương tiện khác. Kỹ thuật giấu tin trong video sẽ sử dụng các vật chứa là các file video. Liên quan đến file video sẽ có rất nhiều định dạng và các chuẩn khác nhau. Chính vì vậy các kỹ thuật giấu tin trong video khi thực hiện giấu tin phải kiểm tra và lựa chọn định dạng file video cho phù hợp và dung chuẩn. Dưới đây bài giảng cung cấp một số định dạng và chuẩn của file video đang được sử dụng phổ biến hiện nay [25]:

a) 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 Multimedia. 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 Multimedia 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. **Chuẩn H.264** là một chuẩn mã hóa/giải mã video và định dạng tệp video đang được sử dụng rộng rãi nhất hiện nay 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.

b) AVI

Định dạng AVI (Audio Video Interle) là một định dạng số đa phương tiện do Microsoft giới thiệu vào tháng khoảng 11/1992 như một chuẩn video dành cho Windows. Tệp AVI có thể chứa cả dữ liệu âm thanh và video trong một tệp, cho phép đồng bộ với phát lại audio – video. Đặc điểm của tệp AVI là dạng video không nén.

c) FLV

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

d) H.263

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

e) WMV

Định dạng WMV (Windows Media Video) là một định dạng video chứa video được mã hóa theo bộ code Windows Media Video và âm thanh được mã hóa theo codec Windows Media Audio codec.

f) 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.

g) 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) H.265

Định dạng H.265 hay còn gọi là HEVC (High Efficiency Video Coding – code video hiệu suất cao) là một định dạng video mang lại khả năng nén cao gần gấp đôi so với H.264/AVC. 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

Do sự phong phú và đa dạng về định dạng file video cũng như khả năng có thể giấu tin trong cấu trúc của một file video nên hiện nay đang có rất nhiều kỹ thuật giấu tin được nghiên cứu và áp dụng vào môi trường video. Theo thống kê từ các tài liệu [1, 14, 24] thì có thể phân loại các kỹ thuật giấu tin trong video thành một số kỹ thuật sau:

a) Phân loại giấu tin trong video 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.

b) Phân loại giấu tin theo miền giấu

- Giấu thông tin trên miền hình ảnh của video.
- Giấu thông tin trên miền âm thanh của video.

c) Phân loại giấu tin theo mục đích

- Thủy vân số:
 - Giấu thông tin vào sự thay đổi khung cảnh
 - Giấu thông tin trong video chuẩn H.264, H265...
 - Giấu thông tin trong miền hệ số.
- Giấu tin mật:

- Giấu thông tin trong mặt phẳng bit.

Dựa vào thống kê về những nghiên cứu trong lĩnh vực giấu tin trong video cũng như những phương pháp giấu tin trong video đang được áp dụng và triển khai trong thực tế hiện nay thì rõ ràng ứng dụng và tiềm năng của các kỹ thuật giấu tin trong video là rất lớn. Tiếp theo, bài giảng sẽ trình bày chi tiết về một số kỹ thuật giấu tin đã được nghiên cứu và áp dụng hiện nay.

4.2. Phương pháp giấu tin trong video

Trong phần 4.1.3 bài giảng đã trình bày tổng quát về một số kỹ thuật giấu tin đang được sử dụng trong lĩnh vực giấu tin trong 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, bài giảng sẽ đi vào trình bày chi tiết một số thuật toán và phương pháp giấu tin trong video.

4.2.1. Phương pháp phát hiện thay đổi khung cảnh

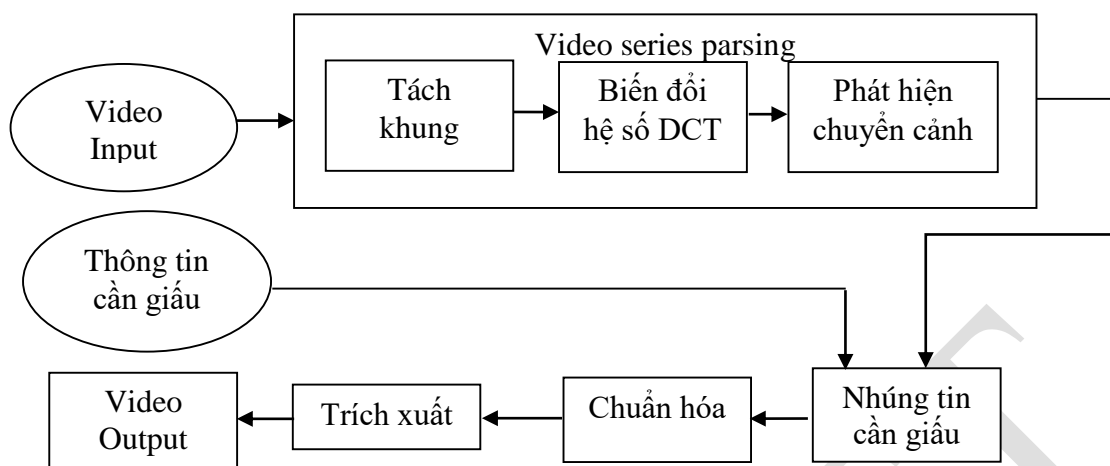
a) Tổng quan chung

Phương pháp giấu tin trong video trên cơ sở phương pháp phát hiện chuyển cảnh là phương pháp giấu tin vào các khung hình của video. Phương pháp này dựa vào sự thay đổi các khung cảnh trong video để giấu thông tin. Cảnh được định nghĩa là những bức hình liên tục chứa các đối tượng (vật thể trên cảnh đó), với mỗi khung hình liên tục thì một cảnh sẽ bao gồm những đối tượng đó. Bình thường video sẽ phân thành các shots. Mỗi shots sẽ thể hiện một sự kiện hay hành động. Trình tự của các khung hình sẽ sắp xếp theo việc ghi hình và chỉnh sửa. Sự khác biệt giữa các khung sẽ đều chỉ ra các điểm chuyển cảnh. Trong chuyển cảnh sẽ bao gồm 2 loại [24]:

- Chuyển cảnh đột ngột (nhảy): 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.

b) Quy trình giấu tin

Các kỹ thuật chuyển cảnh trên rất khó có thể phát hiện bằng mắt thường. Có nhiều phương thức có thể phát hiện được sự chuyển cảnh ví dụ như: dựa vào biểu đồ màu sắc, hệ số DCT,... Sau đây bài giảng sẽ trình bày về thuật toán phát hiện chuyển cảnh dựa vào hệ số DCT. Hình 4.1 trình bày tổng quan về quy trình giấu tin dựa trên sự thay đổi khung cảnh.



Hình 4.1. Quy trình giấu tin trong video dựa trên kỹ thuật phát hiện chuyển cảnh

Việc 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. Sau đó từ những hệ số đã biết của các khối trên những khung hình, sẽ tiến hành phát hiện chuyển cảnh (detect scene change).
- 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 frames chuyển cảnh nào, từ những frames 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 thì 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 bài giảng 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:

$$D(f_k, f_{k+1}) = \sum_u \sum_v [C_k(u, v) - C_{k+1}(u, v)](*)$$

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 pixel 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 pixel 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 đây.

✓ 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. Hệ số DCT của video được sử dụng để tăng tính bảo mật của thông tin được nhúng. Quy trình giấu tin bằng kỹ thuật LSB đã được trình bày trong chương 2 của bài giảng.

✓ Chuẩn hóa

Quá trình chuẩn hóa bao gồm việc kết hợp kết quả của việc phân tích sóng ngắn của phiên bản chuẩn hóa 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 pixel của video (trong dạng số nguyên), từ 0-255, chỉ còn nằm trong khoảng 0 đến 1 của giá trị pixel chuẩn hóa. Mục đích của việc này là đảm bảo các giá trị pixel 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 một 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

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

Trong đó:

- $C_{(p,q)}$ là hệ số DWT của ảnh trong video gốc.
- p, q chỉ các cột và hàng của pixel 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. 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 đã thỏa thuận chọn lựa các khung cảnh cùng với ngưỡng phát hiện chuyển cảnh. Người kiểm tra sẽ thực thi quá trình khôi phục tin mật với mỗi chuyển cảnh họ phát hiện để kiểm tra xem có đúng là tin mật đã được đăng ký không. Thuật toán tách tin như sau

- Các cảnh trong video giấu tin làm đầu vào
- Mỗi khung cảnh được phân tích để thu hệ số DC
- Phát hiện chuyển cảnh dùng hệ số DC
- Từ hệ số phát hiện, các bits thông tin giấu được tách ra. Quá trình tách khôi phục tin nhắn được giấu HM_k bằng công thức:

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

Trong đó:

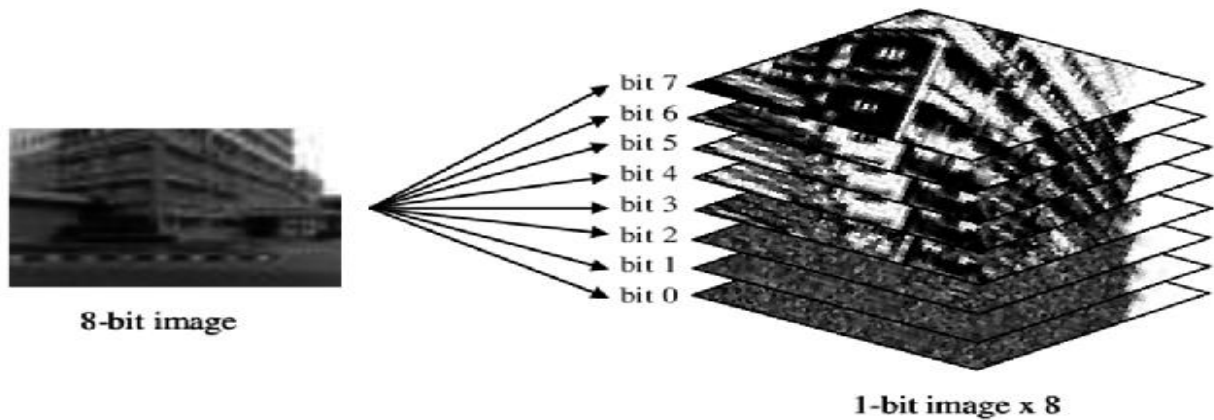
- $S_{k(p,q)}$ là khung video giấu tin;
- $C_{k(p,q)}$ là video gốc;
- k là số khung;
- δ_k là yếu tố để điều chỉnh tính bền vững của video giấu mà đã sử dụng để đổi lại tính vô hình, sự bền vững và tính bí mật. Nếu như điểm chuyển cảnh lớn hơn 0 và bất cứ chuyển cảnh nào diễn ra trong các khung cảnh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

4.2.2. Phương pháp mặt phẳng bit

a) Giới thiệu

Bit Plane Complexity Segmentation steganography (BPCS): phương pháp giấu tin trong mặt phẳng bit là phương pháp giấu tin trong video dựa trên sự biến đổi các khung hình của video. BPCS là các mặt phẳng bit trong mỗi khung hình của video [24, 27].

Mặt phẳng bit: Dựa trên độ sâu màu của điểm ảnh. Giả sử một khung hình ($n \times n$ pixel) 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 4.2 dưới đây biểu diễn bit điểm ảnh thành mặt phẳng bit.



Hình 4.2. Biểu diễn 1 điểm ảnh bit thành 8 mặt phẳng bit

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 8×8 pixel 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:

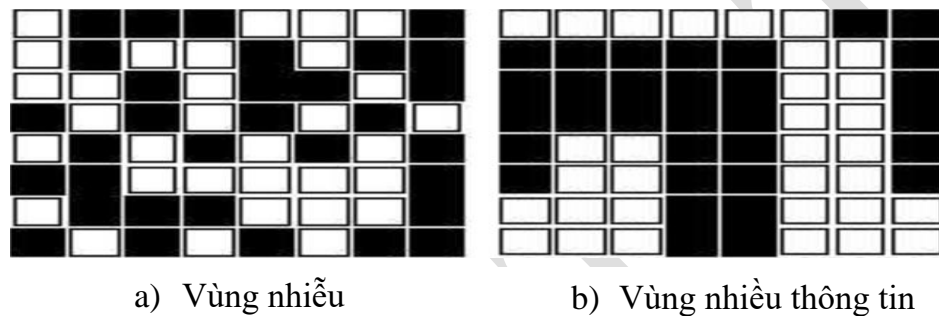
- + Mặt phẳng bit thứ nhất tại (0,0) là ô màu đen (giá trị 0).
- + Mặt phẳng bit thứ hai tại (0,0) là ô màu trắng (giá trị 1).
- +
- + Mặt phẳng bit thứ 8 tại (0,0) là ô màu đen (giá trị 0).

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: 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.
- Khối nhiễu 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.

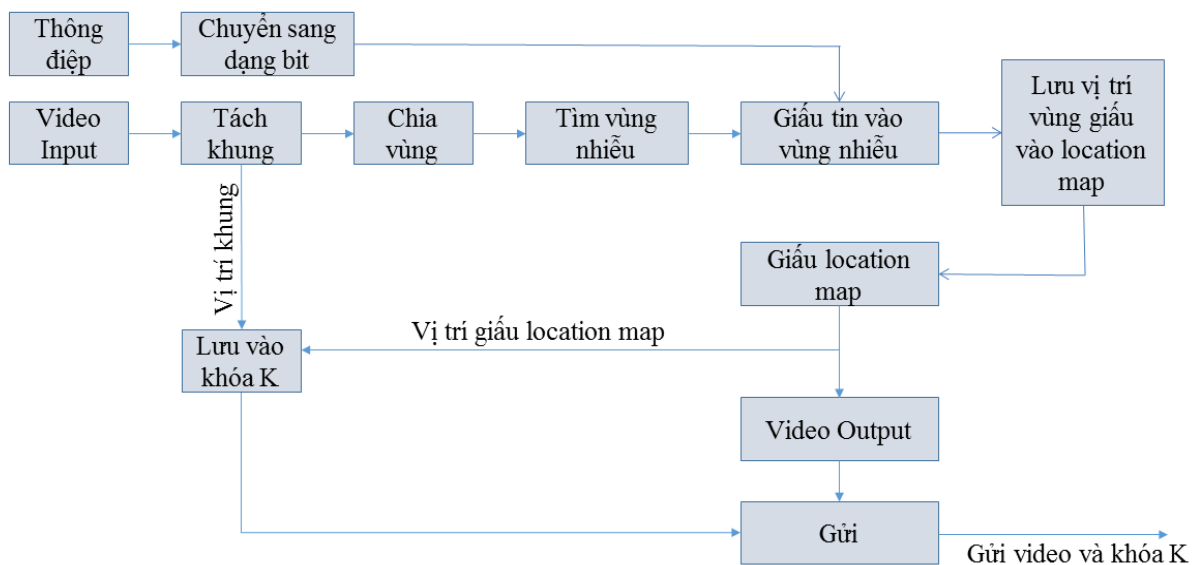
- **Khối nhiễu:** là vùng có độ phức tạp cao hơn ngưỡng phức tạp. Đây là vùng để giấu thông điệp vì đây là vùng ít thông tin quan trọng của hình ảnh. Do đó hệ thống thị giác của con người khó phát hiện được sự thay đổi. Nếu thay đổi không làm thay đổi quá nhiều đến chất lượng của hình ảnh. Trong thực tế phải chọn các mặt phẳng bit được gọi là nhiễu để giấu thông điệp vào đó. Ví dụ về vùng nhiễu và vùng nhiễu thông tin được giới thiệu như hình 4.3 dưới đây. Trong đó màu trắng là giá trị 1 và màu đen là giá trị 0.



Hình 4.3. Phân loại vùng nhiễu và vùng nhiễu thông tin

Từ quy tắc tính như trên có thể thấy: Đối với hình a được coi là vùng nhiễu vì độ phức tạp của mặt phẳng bit là 69. Đối với hình b được coi là vùng nhiễu thông tin vì độ phức tạp của mặt phẳng bit là 29. Như vậy thông tin sẽ được nhúng vào hình 4.3a.

b) Quy trình giấu tin



Hình 4.4. Quy trình giấu tin trong video vào mặt phẳng bit

Từ sơ đồ quy trình giấu tin trong video như hình 4.4 thấy được các bước chính của kỹ thuật giấu tin vào mặt phẳng bit như sau [24, 27]:

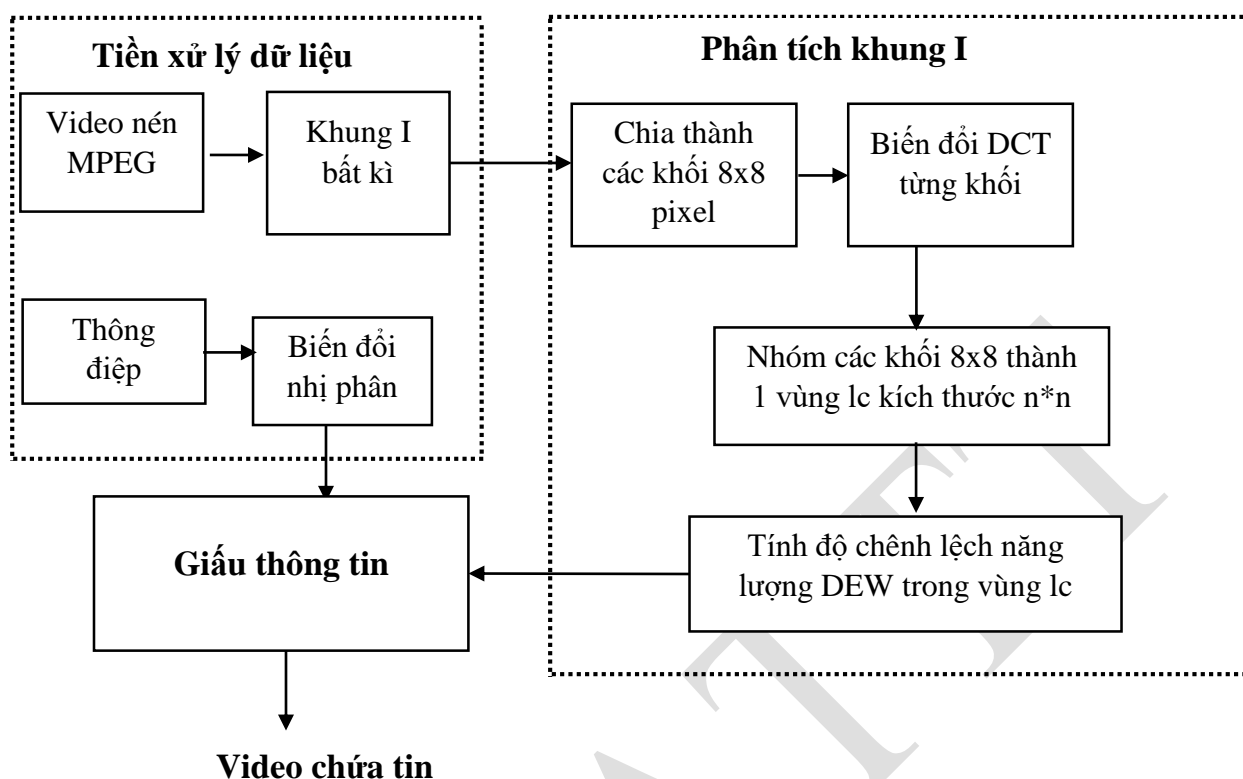
- ✓ Bước 1. Tiền xử lý dữ liệu: với 2 thông tin đầu vào là video input và thông tin mật.
 - Đối với thông tin mật: chuyển thông tin mật thành dạng nhị phân.
 - Đối với video input: tiến hành tách video thành các khung hình. Chọn một khung ảnh bất kì để chuẩn bị giấu thông tin mật. Việc chọn vị trí khung 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.
 - Chia vùng: Sau khi chọn được khung hình sẽ tiến hành chia vùng để tạo thành các mặt phẳng bit. Mỗi pixel có độ sâu màu là 8, 24, 32 bit thì sẽ có 8, 24, 32 mặt phẳng bit tương ứng.
 - Tìm vùng nhiễu: 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 nhiễu thông tin. Quy trình tính toán để xác định vùng nhiễu và vùng nhiễu 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 khóa K cho bên nhận.

4.2.3. 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 giải mã các luồng video hoặc mã hóa lại chúng. Tuy nhiên để nhúng hoặc phát hiện một thủy vân dựa trên mối tương quan thì giải mã MPEG là điều bắt buộc. Điều này có thể quá đòi hỏi quá trình tính toán phức tạp. Ngược lại thấy rằng thuật toán LSB có tính hiệu quả về mặt tính toán cao. Trên thực tế, các ứng dụng đòi hỏi mức độ bảo mật mạng ngang với kỹ thuật nhúng thủy vân dựa trên mối tương quan và có hiệu quả tính toán giống như phương pháp dựa trên LSB. Bởi vậy DEW (Difference Energy Watermarking) được phát triển để thỏa mãn nhu cầu này. DEW có thể áp dụng trực tiếp trên video nén MPEG/JPEG cũng như trên video nguyên thủy.

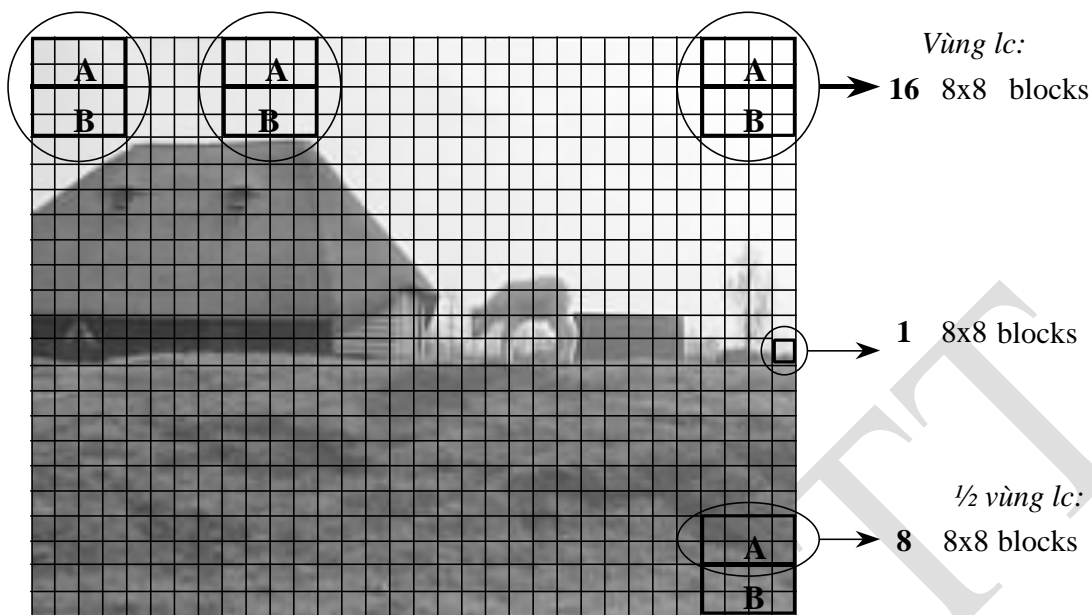
b) Quy trình giấu tin



Hình 4.5. Sơ đồ tổng quát phương pháp giấu tin trong miền video nén dựa bằng DEW

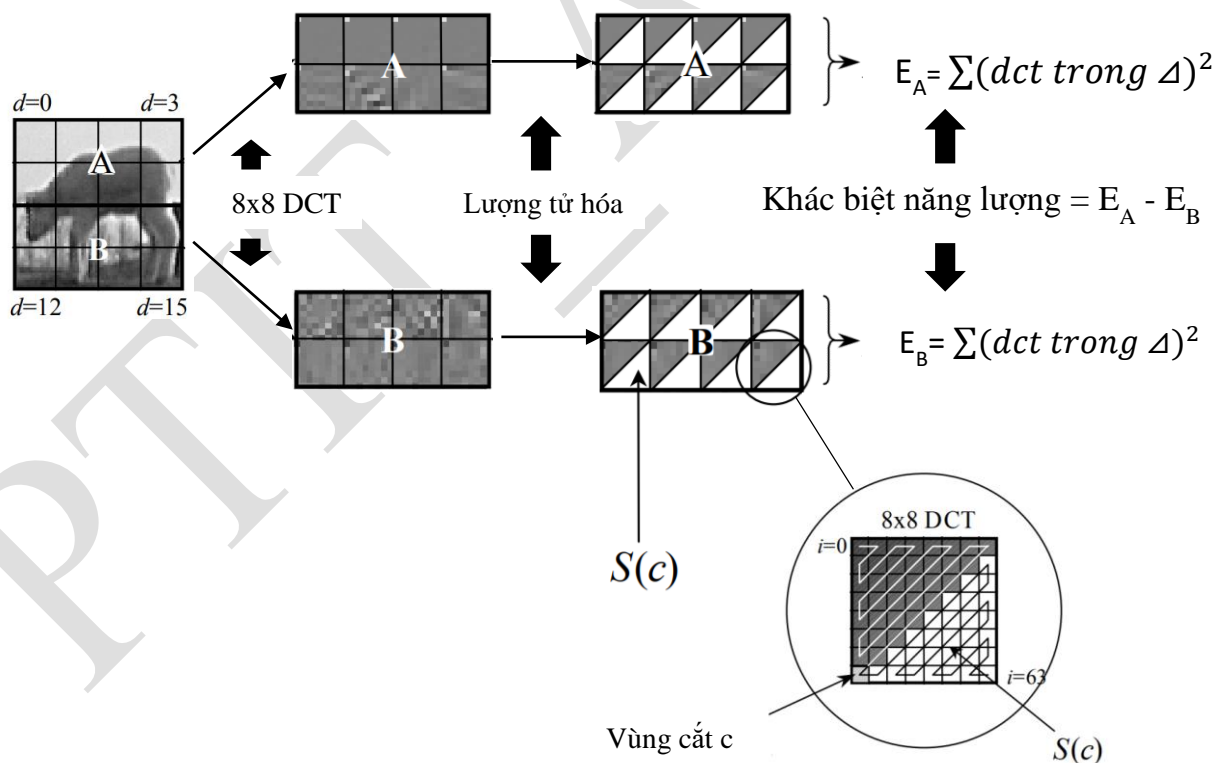
Từ sơ đồ giấu tin trong video theo phương pháp DEW bao gồm các bước sau [1, 24]:

- ✓ 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 4.5 thấy được các bước tiến hành chính trong việc phân tích và xử lý khung hình như sau:
 - Ảnh được chia thành các khối 8×8 pixel. Rồi từ đó đưa về hệ số DCT (các khối 8×8 hệ số DCT).
 - Nhóm các khối 8×8 thành một vùng lc kích thước $n \times n$: Lưu ý: Trong trường hợp trên với $n = 16$ khối 8×8 được gọi là lc -region (khu vực lc). Kích thước của vùng này được gán với giá trị tương ứng trên nhãn. Một lc -region được chia đều thành hai phần A, B mỗi phần tương ứng 8 khối 8×8 DCT. Hình 4.6 mô tả ví dụ về việc chia khối lc .



Hình 4.6. Ví dụ về việc chia khối lc

- Tính độ chênh lệch năng lượng DEW trong vùng lc:



Hình 4.7. Quá trình tính toán năng lượng trong vùng lc

Giải thích các thành phần trong sơ đồ 4.7:

+ 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. Sự khác biệt được định nghĩa theo công thức:

$$D = E_A - E_B;$$

+ Tập con này biểu diễn bởi $S(c)$ (hình tam giác trắng trong hình 4.6). Công thức tính năng lượng tại một vùng như sau:

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

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).

✓ Bước 3: giấu thông tin: 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 “cut-off index c ” của vùng B được loại bỏ bằng cách đặt hệ số DCT tương ứng bằng 0. Khi đó:

$$D = E_A - E_B = E_A - 0 = +E_A$$

- Nếu bit “1” được nhúng, tất cả năng lượng trong vùng “cut-off index c ” của vùng A được loại bỏ. Khi đó

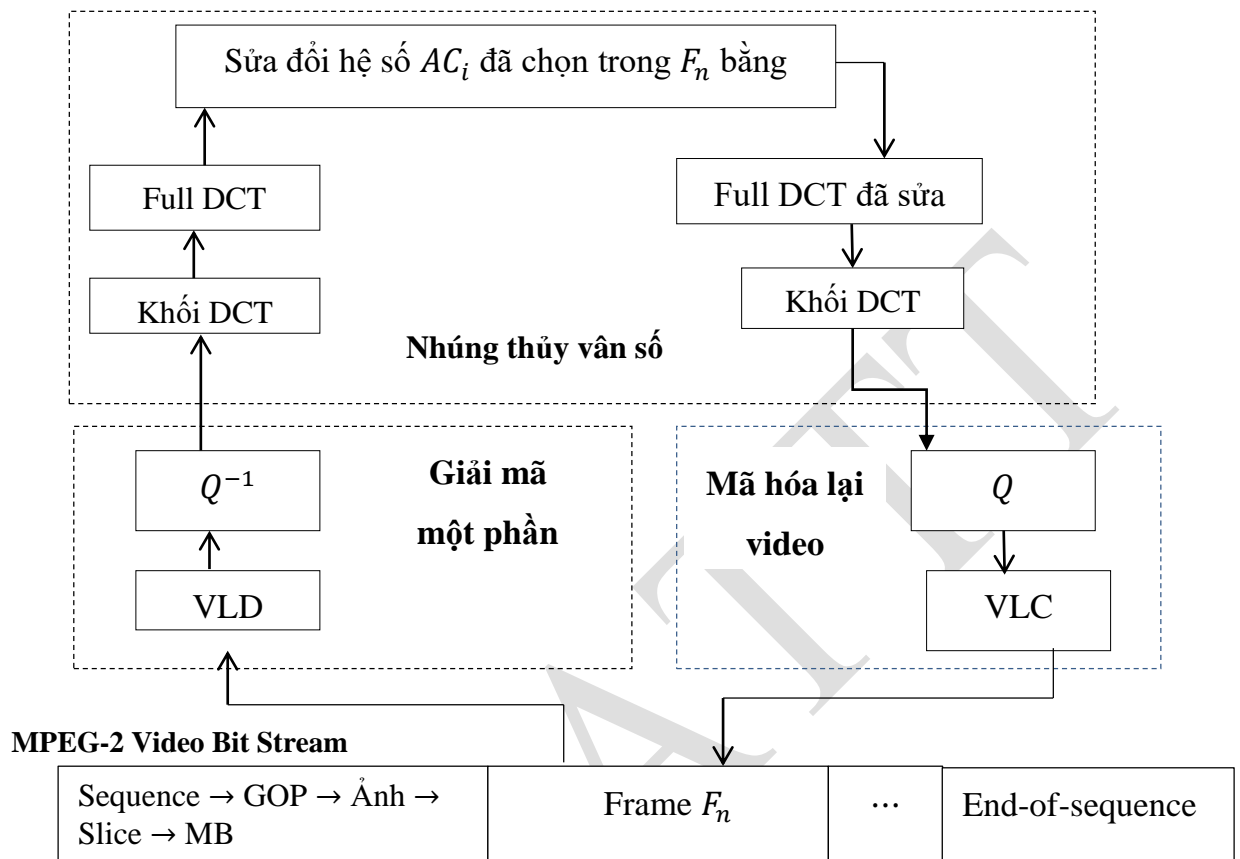
$$D = E_A - E_B = 0 - E_B = -E_B$$

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 block 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 $i=36$.

Vì bit nhúng là 0 nên $D > 0$. Vậy năng lượng E_B cần phải loại bỏ. Nguyên tắc loại bỏ là loại bỏ các hệ số DCT không bằng 0 từ vị trí thứ 35-63 trong vùng B.

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



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

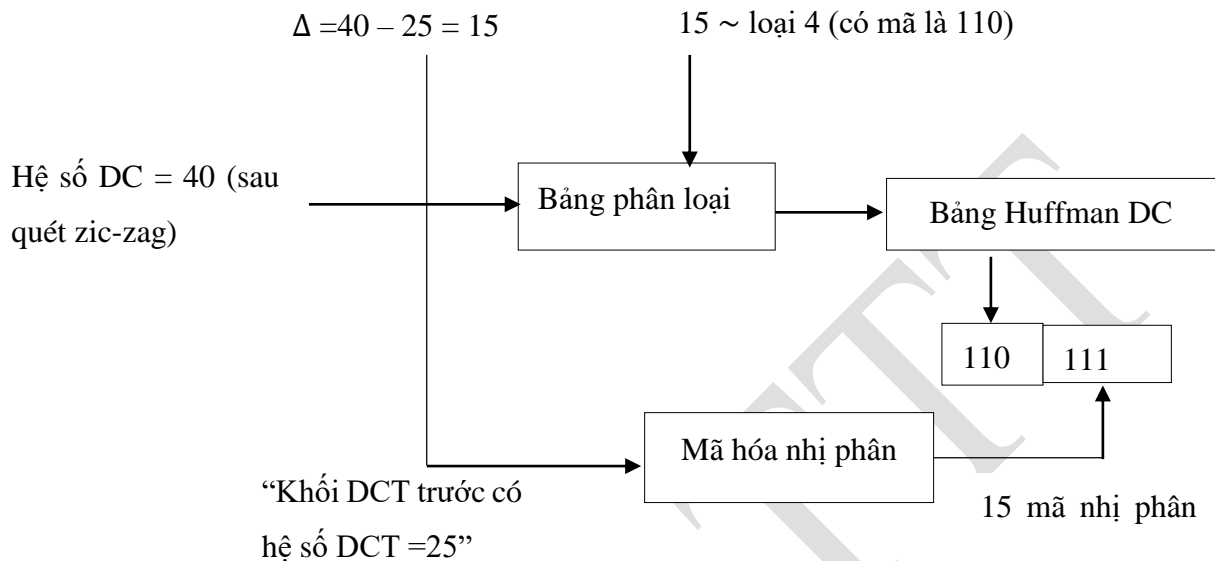
Từ quy trình giấu tin trong video thể hiện trên hình 4.8 thấy được các bước chính trong kỹ thuật giấu tin trên miền nén của video chất lượng cao như sau [1, 24]:

Bước 1. Lựa chọn khung: Chọn một khung bất kỳ để tiến hành nhúng, 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.

Bước 2. Giải nén một phần video: sử dụng khung đã chọn ở bước 1. Việc giải nén một phần của video sử dụng phương pháp chính là VLD (Variable Length Decoding- mã hóa có độ dài biến đổi được) và giải lượng tử hóa. Quy trình thực hiện của các phương pháp này như sau:

- **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. Quá trình mã hóa này được tiến hành trên tất cả các thành phần của hệ số DCT:

✓ 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). Đây là ví dụ về các bước mã hóa entropy thành phần hệ số DC:

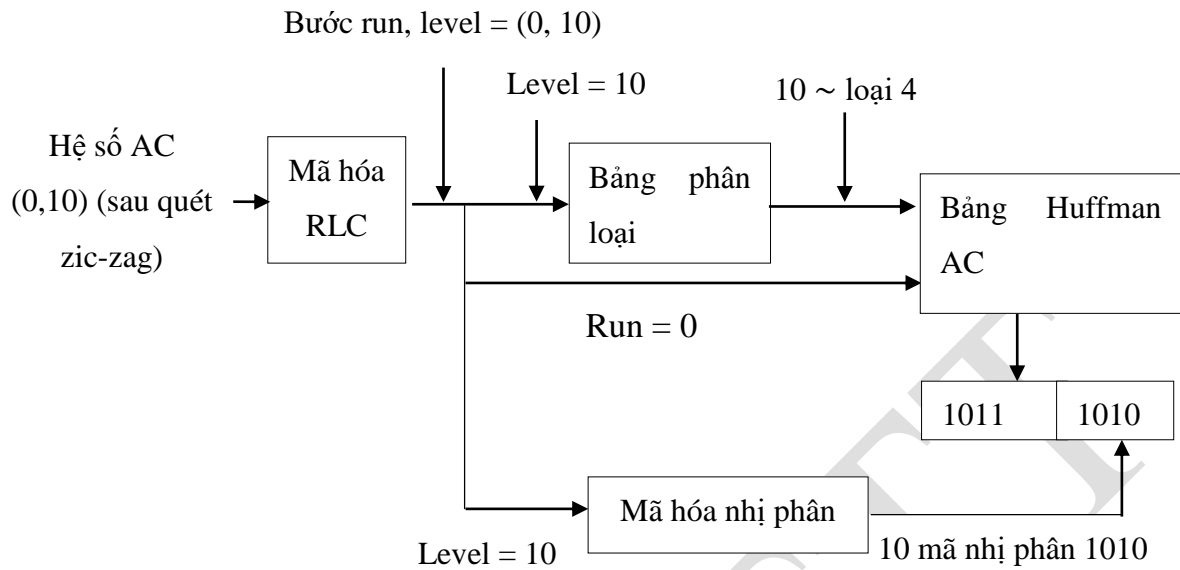


Hình 4.9. Quy trình mã hóa entropy thành phần hệ số DC

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) như ở 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 run	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:** 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 $0 \leq u, v \leq 7$. 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 bài giảng 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.
- ✓ 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: Để có thể giấu được thông tin vào khung hình vừa lựa chọn. Tại đây người giấu tin cần thực hiện các biện pháp tiền xử lý như sau:

- *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 pixel. Ở giai đoạn này người giấu tin cần thực hiện tính toán các DCT toàn khung hình từ khối hệ số DCT 8x8 pixel vừa thu được. Hệ số DCT đầy đủ được tính như sau: 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.

$$FullDCT = \sqrt{\frac{1}{LM}} A_1 \cdot \begin{pmatrix} B_{0,0} & B_{0,1} & \cdots & B_{0,M-1} \\ B_{1,0} & B_{0,2} & \ddots & B_{1,M-1} \\ \vdots & \vdots & \ddots & \vdots \\ B_{L-1,0} & B_{L-1,1} & \cdots & B_{L-1,M-1} \end{pmatrix} \cdot A_2^T$$

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 khoảng vùng.

A_1 và 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:

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

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

Trong đó:

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

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

- *Giai đoạn 2: Điều chỉnh chỉ số lượng tử hóa:* Sử dụng phương pháp điều chỉnh chỉ số lượng tử hóa (QIM) để giấu thông tin vào các hệ số tần số thấp của hệ số DCT toàn khung hình. Để thực hiện được nhiệm vụ này cần thực hiện các quá trình tính kích thước bước Q. Trong thực tế, quá trình tính toán kích thước bước Q áp dụng công thức dưới đây:

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

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_{2n}^2 : 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 dưới đây tạo ra các giá trị thay thế có khoảng cách tối thiểu giữa giá trị gốc và giá trị được sửa đổi:

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

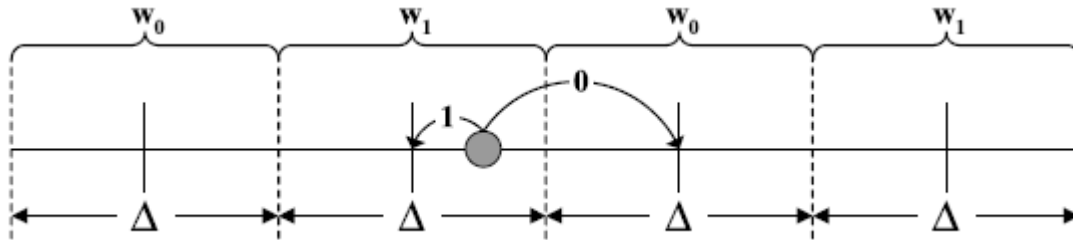
trong đó:

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 dưới đây:

$$d(x_k, w_k) = \begin{cases} \frac{\Delta}{2} & \text{if } (R \bmod 2 = 0, w_k = 0) \text{ or } (R \bmod 2 = 1, w_k = 1) \\ -\frac{\Delta}{2} & \text{if } (R \bmod 2 = 0, w_k = 1) \text{ or } (R \bmod 2 = 1, w_k = 0) \end{cases}$$

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



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

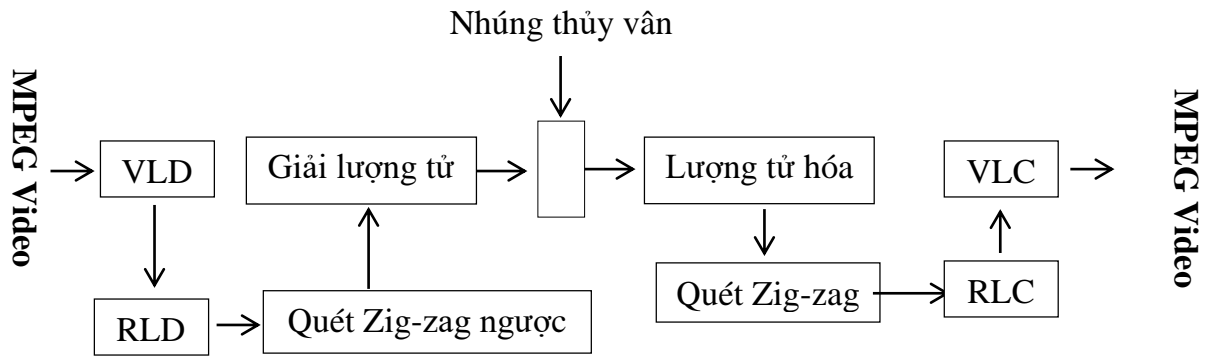
Giấu thông tin bằng cách sử dụng QIM được mô tả trong hình 4.11. Giả sử rằng vòng tròn màu xám là giá trị hệ số ban đầu. Nếu một bit thông tin cần giấu là “1” được nhúng vào hệ số này, nó được thay thế cho giá trị trung bình của w_1 là giá trị gần nhất với giá trị hệ số ban đầu. Nếu một bit thông tin 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 pixel các hệ số DCT. Trong giai đoạn biến đổi DCT ngược chính là cần phải tính toán các khối hệ số DCT nghịch đảo. Trong chương 2 của bài giảng đã trình bày chi tiết về quá trình tính toán DCT ngược.

Bước 4: Mã hóa video: Sau khi đã tính toán các khối hệ số DCT nghịch đảo, 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.

4.2.5. 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

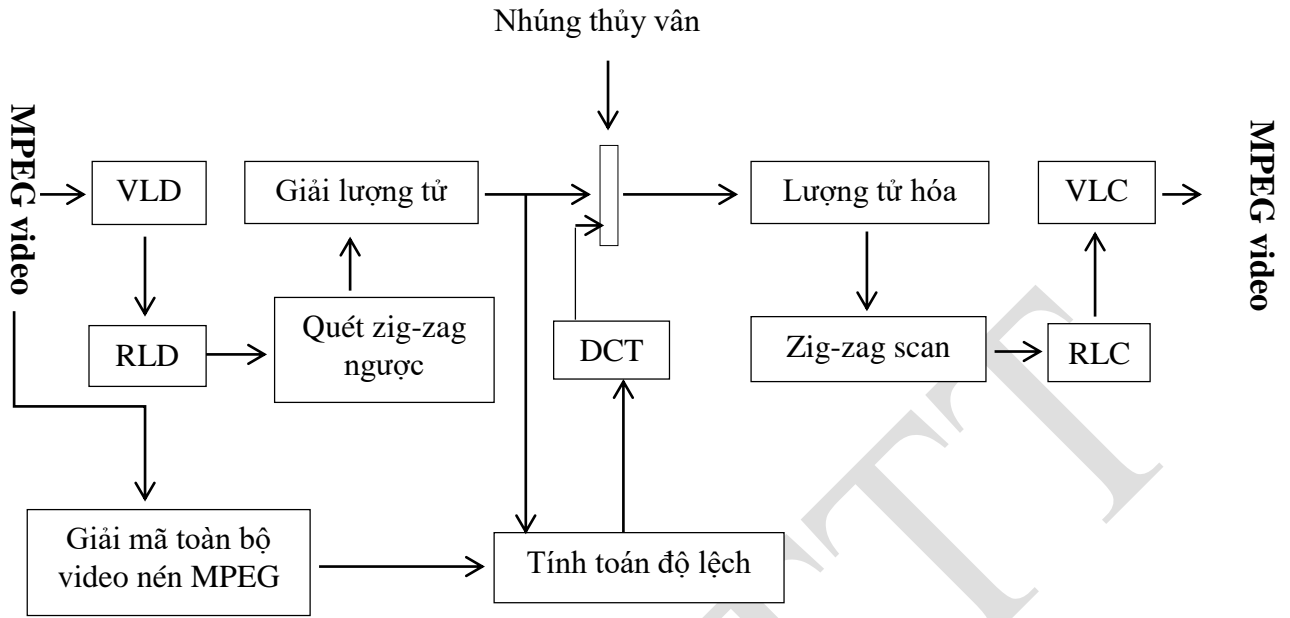
Giải thích các thành phần trong hình 4.12 [24]:

- Đầu vào là video nén chuẩn 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 4.2.4.
- RLC/RLD – Run-level coding/ decoding (mã hóa/ giải mã cấp độ): Ở bước mã hóa cấp độ, đầu vào là block 8x8 DCT sau khi đã được quét zig-zag. Nhiều vị trí trong khối 8x8 có giá trị bằng 0, đặc biệt là các vị trí ứng với các thành phần tần số cao. 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 4.7 và 4.8).
- Các quá trình Quét Zig-zag ngược; giải lượng tử; lượng tử hóa; Quét Zig-zag; VLC đã đều được định nghĩa ở phần 4.2.4.

Trong thực tế để giấu tin mật vào miền hệ số của video thì có nhiều cách khác nhau. Tiếp theo bài giảng sẽ trình bày 2 cách cơ bản nhất và đang được ứng dụng nhiều hiện nay.

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 thông 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 rất nhạy cảm với hệ Y, ít nhạy cảm hơn nhiều với hệ U, V.



Hình 4.14. Quy trình giấu tin trong video bằng 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 . 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:*

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

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:

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

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 $I_{w_{x,y}}(i)$ được xác định bằng cách sử dụng các bảng VLC-B.14 và B.15 của tiêu chuẩn MPEG-2. Nếu kích thước của VLC mã hóa các hệ số DCT là 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:

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

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

- *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. Phương trình tính toán hệ số DCT biến đổi thành:

$$- I_{W_{x,y}}(i) = I_{x,y}(i) + W_{x,y}(i) + Dr_{x,y}(i) \quad \text{với } i \neq 0$$

4.3. Phương pháp phát hiện giấu tin trong video

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

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

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

Trong đó:

x_i biểu thị giá trị tín hiệu gốc

y_i biểu thị giá trị tín hiệu đã bị biến đổi

N là độ dài của tín hiệu âm thanh.

Đối với PSNR: PSNR có đơn vị là deciben (dB), thường được sử dụng trong xử lý tín hiệu số. Công thức tổng quát của PSNR như sau:

$$PSNR = 10 \cdot \log_{10} \left(\frac{\max(x_i)^2}{MSE} \right)$$

Liên quan đến vấn đề phát hiện giấu tin trong video hiện nay đang có một số hướng nghiên cứu và phát hiện giấu tin như sau [32]:

- Phát hiện giấu tin sử dụng phương pháp phân tích sự tăng hình của thông tin giấu: kỹ thuật này được thực hiện bằng cách so sánh các khung hình video gốc và các khung hình của

video đã giấu tin. Chính vì vậy, khi các thuật toán giấu tin ra đời thì các chuyên gia sau khi giấu tin xong đều phải đo lường tính vô hình trước tri giác con người. Một trong những công thức có thể áp dụng chính là PSNR. Giá trị PSNR tối thiểu là 38 dB được chấp nhận làm thước đo chất lượng đối với hình ảnh khung hình của video giấu tin.

- Phát hiện giấu tin sử dụng phương pháp phân tích biểu đồ khung hình: kỹ thuật này được thực hiện bằng cách so sánh biểu đồ của khung trước và sau khi nhúng để biết sự thay đổi về độ phân phối màu pixel do thuật toán giấu tin sử dụng.

- Phát hiện giấu tin sử dụng phương pháp tính toán tỷ lệ lỗi bit (BER): Phương pháp tính toán này cho biết số lượng bit tin thông tin mất tồn tại và được trích xuất thành công từ video có chứa thông tin. BER được định nghĩa là tỷ lệ giữa số lượng các bit được trích xuất sai và tổng số bit tin nhắn ban đầu. Phương trình $BER = \text{Đếm số bit lỗi} / \text{Số lượng bit tin gốc}$.

- Phát hiện giấu tin sử dụng phương pháp tính toán độ bền khi nén: Vì một video không nén có kích thước rất lớn nên nó phải được nén trước khi truyền. Điều này dẫn đến các chuyên gia phải quan tâm đến việc kiểm tra độ bền của video giấu thông tin khi bị nén. Điều này thường được thực hiện bằng cách nén các video giấu thông tin bằng cách sử dụng các kỹ thuật nén khác nhau và với tốc độ nén khác nhau, để biết tỷ lệ sống sót của các bit ẩn.

- Phát hiện giấu tin sử dụng phương pháp tấn công hình học: Đây là kỹ thuật mà kẻ tấn công có thể sử dụng các kỹ thuật như dịch, xoay, cắt xén, làm mờ, khung hình và giảm khung gây ra sự thay đổi lớn đối với cấu trúc và định dạng của video chứa tin mật. Kỹ thuật này có thể sẽ không giúp cho kẻ tấn công thu được thông tin mật nhưng cũng làm cho người nhận không thể trích xuất được thông tin mật khi mà video chứa tin đã bị tấn công.

- Một số kỹ thuật phát hiện khác được đề xuất như: phương pháp phát hiện giấu tin sử dụng mạng nơron và máy hỗ trợ vector(SVM) để phát hiện dữ liệu ẩn bằng cách xem xét miền không gian và thời gian dư thừa. Phương pháp phát hiện giấu tin trong video dựa trên kỹ thuật trải phổ. Mô hình của phương pháp mô phỏng video ban đầu và dữ liệu ẩn độc lập và sử dụng hàm xác suất khối dựa trên tín hiệu khác biệt giữa các khung hình nhằm để lộ hiệu ứng răng cưa (biến dạng) gây ra bằng cách nhúng dữ liệu....

4.4. 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. 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 đổi hệ số AC?
- Câu 7. Hãy trình bày về phương pháp giấu tin trong video sử 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 đổi hệ số DC?
- Câu 8. 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 9. 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 10. Hãy trình bày về một số phương pháp phát hiện giấu tin trong video?

CHƯƠNG 5: GIẤU TIN TRONG VĂN BẢN

Trong chương trình bày một số kiến thức liên quan đến kỹ thuật giấu tin trong văn bản 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. Ngoài ra, chương 5 đề cập đến một số phương pháp, kỹ thuật phát hiện giấu tin trong văn bản

5.1. Đặc điểm của giấu tin trong văn bản

5.1.1. Giới thiệu chung

Phương pháp giấu tin trong văn bản này dựa vào các đặc điểm của văn bản để giấu thông tin mật vào trong văn bản ví dụ như: các dòng văn bản hay khoảng cách giữa các từ khóa. Tuy nhiên điểm yếu của giấu tin trong văn bản là ít có thông tin dư thừa, muốn thực hiện giấu tin cần khéo léo khai thác các dư thừa tự nhiên của ngôn ngữ. Các kỹ thuật giấu tin trong văn bản cũng vẫn đảm bảo được các yêu cầu cần thiết của văn bản sau khi giấu cũng như mục đích của việc thông tin giấu. Giấu tin trong văn bản là một trong những phương pháp đang được áp dụng và triển khai nhiều trong thực tế hiện nay.

5.1.2. Một số định dạng văn bản điển hình

a) Các loại bảng mã

Về bản chất, máy tính chỉ làm việc với các con số, do đó để biểu diễn các ký tự trên máy tính cần phải có một quy ước nhất quán giữa các ký tự cần biểu diễn và các con số tương ứng để máy tính có thể hiểu và xử lý. Quy ước này được thể hiện qua các bước:

- Chọn tập các ký tự cần mã hóa
- Gán cho mỗi ký tự cần mã hóa một giá trị nguyên không âm, gọi là *điểm mã*.
- Chuyển các điểm mã thành dãy các *đơn vị mã* để phục vụ cho việc lưu trữ và mã hóa. Các điểm mã không nhất thiết phải có cùng số đơn vị mã.

Tập hợp những điểm mã của một tập các ký tự được gọi là *bảng mã*. Như vậy khi nói về một bảng mã, chỉ quan tâm đến hai điều là số lượng các ký tự được mã hóa, và cách mã hóa chúng thành các đơn vị mã.

- *Bảng mã ASCII*: ASCII (American Standard Code for Information Interchange - Chuẩn mã trao đổi thông tin Hoa Kỳ) là bộ kí tự và bộ mã kí tự đầu tiên lúc máy tính được phát minh, dựa trên bảng chữ cái La Tinh được dùng trong tiếng Anh hiện đại và các ngôn ngữ Tây Âu khác. Bảng mã ASCII chuẩn có 128 kí tự, các điểm mã có giá trị nằm trong

khoảng từ 0-127, gồm các kí tự điều khiển, các ký tự in được như bảng chữ cái, các dấu. Bảng mã ASCII mở rộng có 256 kí tự gồm 128 ký tự của bảng mã ASCII chuẩn và các chữ có dấu, ký tự trang trí, v.v...

- *Bảng mã Unicode*: Unicode là bộ mã chuẩn quốc tế được thiết kế để dùng làm bộ mã duy nhất cho tất cả các ngôn ngữ khác nhau trên thế giới, kể cả các ngôn ngữ sử dụng ký tự tượng hình phức tạp như tiếng Trung Quốc, Thái Lan,... Unicode thống nhất chung các ký tự của mọi ngôn ngữ trong một bảng mã duy nhất. Unicode cung cấp một biểu diễn số duy nhất cho mỗi một ký tự và không quan tâm đến nền tảng, chương trình hay ngôn ngữ là gì.

b) Một số loại văn bản điển hình

- *Văn bản text*: Văn bản text hay văn bản thuần túy (Plain text, trái với Formatted text, styled text hay rich text) là dạng trình bày văn bản trên máy tính chỉ chứa văn bản mà không sử dụng các định dạng văn bản để trình bày, nó có thể đọc được dễ dàng mà không cần xử lý phức tạp. Hầu hết các tệp văn bản thuần túy đều có phần mở rộng là đuôi *.txt* và có rất nhiều các phần mềm hỗ trợ việc soạn thảo văn bản thuần túy sẵn có trên hệ điều hành như là Notepad, NotePad++ (Windows), edit (DOS), ed, emacs, vi, vim, Gedit hoặc nano (Unix, Linux), SimpleText (Mac OS), hoặc TextEdit (Mac OS X).

- *Siêu văn bản HTML*: HTML - **H**yper **T**ext **M**arkup **L**anguage (Ngôn ngữ đánh dấu siêu văn bản) được sử dụng để tạo một trang web, trên một website có thể sẽ chứa nhiều trang và mỗi trang được quy ra là một tài liệu HTML. Một tập tin HTML sẽ bao gồm các phần tử HTML và được lưu lại dưới đuôi mở rộng là **.html** hoặc **.htm**. Các thẻ HTML không phân biệt chữ hoa chữ thường và có thể tạo tài liệu HTML bằng bất kỳ trình soạn thảo nào như Notepad, DreamWeaver, ...

- *Văn bản theo chuẩn Microsoft Word*: Microsoft Word, còn biết đến với tên khác là Winword, là một công cụ soạn thảo văn bản khá phổ biến hiện nay của công ty phần mềm nổi tiếng Microsoft. Nó cho phép người dùng làm việc với văn bản thô (text), các hiệu ứng như phông chữ, màu sắc cùng với hình ảnh đồ họa và nhiều hiệu ứng đa phương tiện khác nhau như âm thanh, video khiến cho việc soạn thảo văn bản được sinh động và thuận tiện hơn. Ngoài ra cũng có các công cụ kiểm tra như kiểm tra chính tả, ngữ pháp của nhiều ngôn ngữ khác nhau để hỗ trợ cho người dùng.

- *Văn bản theo chuẩn định dạng PDF*: PDF hay còn được gọi với cái tên đầy đủ

Portable Document Format là một định dạng văn bản di động của hãng Adobe System. Tương tự như Microsoft Word, file PDF hỗ trợ hiển thị nhiều loại nội dung khác nhau như text, hình ảnh, video,... Hơn thế nữa, với ưu điểm nhỏ gọn cùng tính bảo mật cao nên PDF được sử dụng rộng rãi để lưu trữ tài liệu trên mạng. Đặc biệt các định dạng file PDF không thể chỉnh sửa, thay đổi được nội dung mà chỉ có phần mềm chuyên dụng mới chỉnh sửa được. Nhưng khi chỉnh sửa sẽ khó có được văn bản chuẩn như ban đầu.

5.1.3. Phân loại phương pháp giấu tin trong văn bản

Hiện nay, áp dụng trong lĩnh vực giấu tin trong văn bản có nhiều thuật toán và kỹ thuật khác nhau. Một số nhóm thuật toán chính được áp dụng trong lĩnh vực giấu tin trong văn bản như sau [1, 2, 28, 29]:

a) Giấu tin dựa vào định dạng văn bản

Các phương pháp dựa trên định dạng văn bản sẽ sử dụng và thay đổi một số kiểu định dạng của văn bản chứa để ẩn giấu thông tin. Các phương pháp này không thay đổi bất kỳ một từ hay câu nào, do đó không làm ảnh hưởng đến nội dung của văn bản chứa. Đặc điểm của các phương pháp giấu tin dựa trên định dạng văn bản là chỉ có một lượng nhỏ dữ liệu được ẩn trong văn bản và thông tin mật không dễ bị phát hiện bởi con người. Đặc biệt các phương pháp này áp dụng cho tất cả các loại văn bản. Một số phương pháp giấu tin trong văn bản dựa trên định dạng văn bản như:

- Phương pháp sử dụng khoảng trắng.
- Phương pháp dịch chuyển vị trí dòng.
- Phương pháp dịch chuyển vị trí từ.
- Phương pháp thay đổi màu sắc hoặc kích thước của các ký tự.

b) Phương pháp sinh ngẫu nhiên và thống kê

Các phương pháp sinh ngẫu nhiên và thống kê là phương pháp sử dụng các thuộc tính thống kê của ngôn ngữ. Các phương pháp này sử dụng những mẫu ngữ pháp để sinh ra những văn bản chứa tự động bằng một ngôn ngữ tự nhiên hoặc dựa vào các thuộc tính thống kê đó để phân loại nhóm ký tự. Một số phương pháp giấu tin trong văn bản dựa trên phương pháp sinh ngẫu nhiên và thống kê như:

- Phương pháp sử dụng văn phạm phi ngữ cảnh.
- Phương pháp dựa trên tính phản xạ đối xứng của ký tự.

c) Phương pháp sử dụng tính chất ngôn ngữ

Phương pháp này sử dụng các thuộc tính của ngôn ngữ tự nhiên, ví dụ cấu trúc ngôn ngữ để ẩn giấu các thông điệp bí mật. Nhóm các kỹ thuật điển hình trong phương pháp này là:

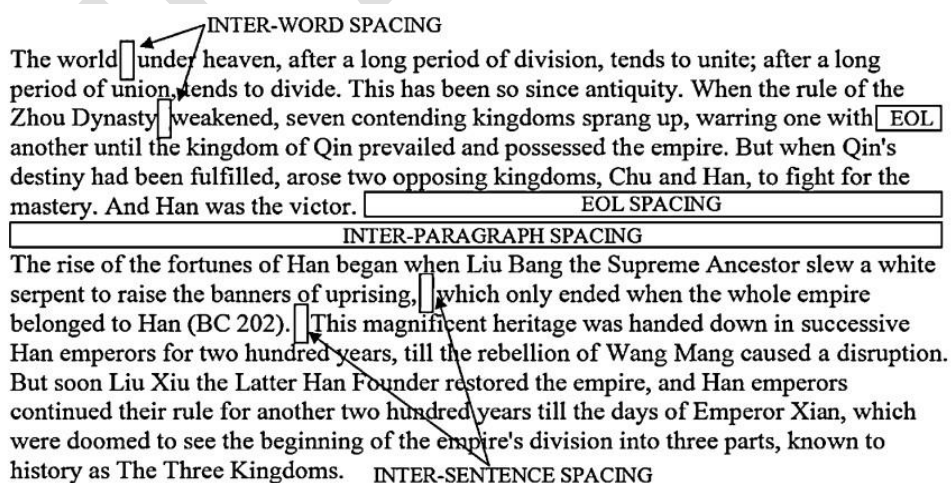
- Phương pháp sử dụng cú pháp.
- Phương pháp sử dụng ngữ nghĩa.

Trên đây bài giảng đã liệt kê một số phương pháp và kỹ thuật chính trong lĩnh vực giấu tin trong văn bản. Từ sự thống kê các phương pháp và thuật toán đang được ứng dụng trong lĩnh vực giấu tin trong văn bản có thể nhận thấy rằng phương pháp giấu tin trong văn bản đang được nghiên cứu và ứng dụng hạn chế. Việc các phương pháp giấu tin trong văn bản chưa được ứng dụng rộng rãi như các phương pháp khác bởi vì 2 lý do chính là đặc thù của định dạng văn bản và đặc tính của các thuật toán. Tiếp theo, để làm rõ hơn đặc tính của các thuật toán, phương pháp giấu tin trong văn bản, bài giảng sẽ mô tả chi tiết các thuật toán giấu tin và tách tin này.

5.2. Phương pháp dựa trên định dạng văn bản

5.2.1. Phương pháp sử dụng khoảng trắng

Khoảng trắng trong văn bản có thể hiểu là khoảng cách giữa các, các câu hoặc các dòng. Trong phương pháp sử dụng khoảng trắng, các khoảng trắng có thể được thêm vào sau mỗi từ, mỗi câu, mỗi đoạn. Hình 5.1 mô tả về một số vị trí khoảng trắng có thể lựa chọn để giấu tin [1, 2, 28, 29].



Hình 5.1. Một số vị trí khoảng trắng có thể lựa chọn để giấu tin

a) Phương pháp sử dụng khoảng trắng giữa các từ

Phương pháp sử dụng khoảng trắng giữa các từ sử dụng một hoặc hai khoảng trắng đặt giữa các từ liên tiếp, với quy ước một khoảng trắng tương ứng với bit 0 và hai khoảng trắng tương ứng với bit 1. Tuy nhiên, một vấn đề có thể xảy ra với phương pháp này là trong trường hợp hai từ cuối của một dòng có duy nhất một khoảng trắng (để căn lề chính xác) nhưng bit cần ẩn dấu lại là bit 1 (yêu cầu hai khoảng trắng). Để giải quyết vấn đề này, một thuật toán sử dụng các khoảng trắng để giấu thông tin được đề xuất như sau:

- Một khoảng trắng + một từ + hai khoảng trắng tương ứng với bit 0 được giấu.
- Hai khoảng trắng + một từ + một khoảng trắng tương đương với bit 1 được giấu.
- Một khoảng trắng + một từ + một khoảng trắng tương đương với không có thông tin được ẩn giấu.
- Hai khoảng trắng + một từ + hai khoảng trắng tương đương với không có thông tin được ẩn giấu.

Từ các quy ước trên dẫn đến kỹ thuật giấu tin và tách tin trong văn bản sử dụng khoảng trắng giữa các từ như sau:

Thuật toán giấu tin:

Đầu vào:

- Thông điệp bí mật
- Văn bản phủ

Các bước thực hiện:

- Bước 1: Chuyển đổi thông điệp giấu thành dạng nhị phân
- Bước 2: Đọc dạng nhị phân của thông điệp bí mật và với mỗi bit nhị phân được

chuyển đổi, thêm các khoảng trắng vào văn bản phủ theo quy ước được mô tả ở trên.

Đầu ra:

- Văn bản phủ có chứa thông điệp bí mật

Để hiểu rõ hơn về phương pháp này, hãy xét ví dụ dưới đây.

Với hai dữ liệu đầu vào là:

- Thông tin bí mật là chữ “H” chuyển sang dạng nhị phân có dạng “01001000”.
- Văn bản gốc:

Happy families are all alike every unhappy family is unhappy in its own way everything was in confusion in the Oblonskys house.

Áp dụng nguyên tắc giấu tin trong văn bản sử dụng khoảng trắng giữa các từ thì thu được văn bản chữ tin mật như sau:

Happy families are all alike every unhappy family is unhappy in its own way everything was in confusion in the Oblonskys house.

Nhận xét: từ bản bản được giấu tin thấy được rằng, văn bản sau khi giấu tin nếu có độ rộng khoảng trắng giữa 02 từ là đủ lớn thì có thể quan sát được bằng mắt thường, chính vì vậy, người giấu tin phải định nghĩa lại độ rộng của mỗi khoảng trắng sao cho 02 khoảng trắng trông như 01 khoảng trắng nếu quan sát bằng mắt thường. Đây là phương pháp giấu tin đơn giản và dễ thực hiện. Tuy nhiên, nếu văn bản đã giấu tin được gõ lại bằng tay hoặc được xử lý bởi các trình xử lý tự động loại bỏ khoảng trắng thừa thì thông tin mật sẽ bị hủy. Chính vì vậy phương pháp này không được đánh giá cao và chỉ phù hợp với văn bản in.

b) Phương pháp giấu tin vào cuối mỗi dòng

Nguyên tắc giấu tin vào cuối mỗi dòng dựa trên việc tận dụng các khoảng trắng thêm vào sau mỗi dòng có thể lưu trữ được một lượng lớn các bit. Các khoảng trắng ở cuối mỗi dòng có thể bị bỏ qua và không hiện lên các bởi các ứng dụng đọc văn bản. Trong toàn bộ văn bản, nếu giấu tin vào cuối mỗi dòng thì lượng bit thu được là rất lớn, có thể có đủ không gian để lưu trữ chuỗi bí mật.

Thuật toán giấu tin:

Đầu vào:

- Thông điệp bí mật
- Văn bản phủ

Các bước thực hiện:

- Bước 1: Chuyển thông điệp bí mật thành dạng nhị phân
- Bước 2: Đọc dạng nhị phân của thông tin bí mật và thêm khoảng trắng vào cuối mỗi dòng theo quy ước: 0 dấu cách sẽ tìm đến câu tiếp theo và tương đương không có bit thông tin nào được giấu trong đó; 1 dấu cách sẽ mã hóa 0; 2 dấu cách sẽ mã hóa 1.

Đầu ra:

- Văn bản phủ có chứa thông điệp

Để hiểu rõ hơn về phương pháp này, hãy xét ví dụ dưới đây:

Thông điệp bí mật là chữ “H” chuyển sang dạng nhị phân có dạng “01001000”

Văn bản gốc:

*“Quê hương là một tiếng ve
Lời ru của mẹ trưa hè à ơi
Dòng sông con nước đầy vui
Quê hương là một góc trời tuổi thơ
Quê hương ngày ấy như mơ
Tôi là cậu bé dại khờ đáng yêu
Quê hương là tiếng sáo diều
Là cánh cò trắng chiều chiều chân đề.”*

Văn bản đã giấu tin sử dụng kỹ thuật :

*“Quê hương là một tiếng ve_
Lời ru của mẹ trưa hè à ơi__
Dòng sông con nước đầy vui_
Quê hương là một góc trời tuổi thơ_
Quê hương ngày ấy như mơ__
Tôi là cậu bé dại khờ đáng yêu_
Quê hương là tiếng sáo diều_
Là cánh cò trắng chiều chiều chân đề._”*

Chú ý: (dấu “_” ở đây là dấu cách)

Nhận xét: Thêm một hoặc hai khoảng trắng vào cuối mỗi dòng trong văn bản cũng là một phương pháp giấu tin đơn giản. Những khoảng trắng được thêm vào sẽ không xuất hiện khi văn bản được in ra nhưng có thể dễ dàng bị phát hiện bởi các bộ xử lý và thông điệp bí mật sẽ bị hủy bỏ khi mà văn bản được gõ lại bằng tay hoặc được xử lý bởi một chương trình xử lý tự động loại bỏ khoảng trắng thừa. Chính vì vậy, phương pháp này cũng không được đánh giá cao.

5.2.2. Phương pháp dịch chuyển vị trí dòng

Trong phương pháp này, các dòng của văn bản sẽ được dịch chuyển theo chiều dọc với một độ dài nhất định, ví dụ mỗi dòng sẽ được dịch chuyển một khoảng rất nhỏ khoảng 1/300 inch lên hoặc xuống (inch là một đơn vị chiều dài trong hệ thống đo lường) và thông tin sẽ được ẩn giấu bằng việc tạo ra các hình dạng của khoảng dịch chuyển của văn bản. Thông điệp sẽ được giấu vào khoảng dịch chuyển đó bằng cách chèn vào các bit 0 hoặc 1 tùy theo quy ước. Điều này rất khó có thể phát hiện bằng mắt thường vì khoảng cách thay đổi khá nhỏ.

Thuật toán giấu tin:

Đầu vào:

- Thông điệp bí mật
- Văn bản phủ

Các bước thực hiện:

- Bước 1: Chuyển thông tin bí mật thành dạng nhị phân
- Bước 2: Đọc dạng nhị phân của thông điệp bí mật và dịch chuyển vị trí các dòng theo quy ước dòng được dịch giảm đi tương ứng bit 0 được giấu, dòng được dịch tăng lên tương ứng bit 1 được giấu.

Đầu ra:

- Văn bản chứa thông điệp.

Ví dụ về giấu tin trong văn bản sử dụng kỹ thuật dịch chuyển dòng:

Thông điệp cần giấu là 2 bit “01”

Văn bản gốc:

Dòng bình thường

Dòng bình thường

Văn bản sau khi giấu tin:

Dòng được dịch chuyển giảm đi

Dòng được dịch chuyển tăng lên

↑
h-i

↑
h+i

Nhận xét: trong phương pháp dịch chuyển vị trí dòng khoảng cách có thể được chú ý bằng cách sử dụng các công cụ đánh giá khoảng cách đặc biệt. Ngoài ra nếu văn bản được gõ lại bằng tay hoặc nếu chương trình nhận dạng ký tự được sử dụng, thông tin bí mật sẽ bị phá

hủy. Chính vì vậy phương pháp này chỉ phù hợp với các văn bản in, để tránh thay đổi định dạng của văn bản.

5.2.3. Phương pháp dịch chuyển vị trí từ

Kỹ thuật giấu tin trong văn bản sử dụng phương pháp dịch chuyển vị trí các từ dựa trên cơ chế giống như dịch chuyển vị trí dòng, nhưng người giấu tin thay vì dịch chuyển vị trí của các dòng thì sẽ dịch chuyển vị trí các từ. Sau đó tùy vào khoảng dịch chuyển đó nằm bên trái hay bên phải từ mà quy định nó là bit 0 hay bit 1. Dịch trái sẽ là bit 0 còn dịch phải sẽ là bit 1.

Thuật toán giấu tin:

Đầu vào:

- Thông điệp bí mật
- Văn bản phủ

Các bước thực hiện:

- Bước 1: Chuyển thông tin bí mật thành dạng nhị phân
- Bước 2: Đọc dạng nhị phân của thông điệp bí mật và dịch chuyển vị trí các dòng

theo quy ước dịch trái sẽ là bit 0 còn dịch phải sẽ là bit 1.

Đầu ra:

- Văn bản phủ có chứa thông điệp

Ví dụ:

Thông điệp bí mật là chữ “A” chuyển sang dạng nhị phân có dạng “01000001”

Văn bản gốc và văn bản sau khi giấu tin:

The quick brown fox jumps over the lazy dog.

Văn bản sau khi đã giấu tin là:

The quick brown fox jumps over the lazy dog.

Trong ví dụ trên, dòng thứ nhất các chữ có vị trí không bị thay đổi. Còn dòng thứ 2 các chữ bị dịch trái hoặc phải để mã hóa cho chuỗi 01000001. Độ dịch chuyển là rất nhỏ và nếu không so sánh với chuỗi ban đầu thì khó có thể nhận biết được chuỗi đó có bị thay đổi hay không. Phương pháp này cũng phù hợp với văn bản in và nếu văn bản được gõ lại bằng tay hoặc nếu chương trình nhận dạng ký tự được sử dụng, thông tin bí mật sẽ bị phá hủy.

5.3. Phương pháp sinh ngẫu nhiên và thống kê

5.3.1. Phương pháp sử dụng văn phạm phi ngữ cảnh

Việc ẩn giấu thông tin trong các văn bản nhân tạo phải vượt qua được các cơ chế kiểm tra bằng máy tính. Những văn bản đó phải đáp ứng ít nhất các yêu cầu sau đây [2, 28, 29]:

- Tần suất xuất hiện của các chữ cái trong văn bản phải giống như trong ngôn ngữ tự nhiên. Nếu văn bản sử dụng ngôn ngữ tiếng Anh, chữ E và T phải là những chữ cái thường xuyên xuất hiện nhất, còn Z và Q phải là những chữ cái ít xuất hiện nhất.
- Hầu hết các từ trong văn bản được sử dụng phải là các từ được liệt kê trong các từ điển chính quy. Nếu trong các văn bản có quá nhiều các từ như tên riêng, tiếng lóng hay thuật ngữ khoa học khi bị kiểm tra bởi các máy tính sẽ bị đánh dấu là những văn bản đáng ngờ.
- Các câu trong văn bản phải đúng cú pháp. Nếu một chương trình kiểm tra cú pháp tự động tìm thấy một lỗi cú pháp như hai động từ liên tiếp trong một văn bản thì sẽ bị đánh dấu là một văn bản đáng ngờ.

Phương pháp sử dụng văn phạm phi ngữ cảnh sẽ sử dụng một văn phạm phi ngữ cảnh (CFG - Context Free Grammar) để sinh ra các câu tạo thành văn bản nhân tạo chứa thông điệp bí mật và văn bản này có thể bắt chước các văn bản thực tế (nghĩa là có các thuộc tính thống kê giống nhau). Văn phạm phi ngữ cảnh là một tập hợp hữu hạn các biến (còn gọi là các ký hiệu chưa kết thúc), mỗi biến biểu diễn một ngôn ngữ. Ngôn ngữ được biểu diễn bởi các biến được mô tả một cách đệ quy theo thuật ngữ của một khái niệm khác gọi là ký hiệu kết thúc. Quy tắc quan hệ giữa các biến gọi là luật sinh. Mỗi luật sinh có dạng một biến, ở vế trái sinh ra một chuỗi có thể gồm biến lẫn các ký hiệu kết thúc trong văn phạm. Văn phạm phi ngữ cảnh là một hệ thống gồm bốn thành phần, ký hiệu là văn phạm $G(V, T, P, S)$, trong đó:

- V là tập hữu hạn các biến (hay ký tự chưa kết thúc).
- T là tập hữu hạn các ký tự kết thúc, $V \cap T = \emptyset$
- P là tập hữu hạn các luật sinh mà mỗi luật sinh có dạng $A \rightarrow \alpha$ (với A là biến và α là chuỗi các ký hiệu $\in (V \cup T)^*$)
- S là một biến đặc biệt gọi là ký hiệu bắt đầu văn phạm.

Các quy tắc sau chỉ ra cách để tạo ra một chuỗi (gồm các ký hiệu kết thúc) từ một CFG cho trước:

- Sử dụng một ký hiệu bắt đầu (một ký hiệu chưa kết thúc đặc biệt) để khởi đầu. Chọn một luật có ký hiệu khởi đầu ở bên trái và chọn một ký hiệu ở phần bên phải của luật để thay

thế kí hiệu khởi đầu này. Kí hiệu được sử dụng sẽ là một thành tố của văn bản sẽ được tạo sau này.

- Chọn một kí hiệu chưa kết thúc trong văn bản, tìm một luật có kí hiệu chưa kết thúc này ở bên trái và thay thế kí hiệu này bằng một kí hiệu ở phần bên phải của luật.
- Lặp lại bước 2 cho đến khi văn bản chỉ còn toàn các kí hiệu kết thúc.

Sau đây là một ví dụ của một CFG dùng để giấu chuỗi *0100110* trong đó các kí hiệu chưa kết thúc là các kí hiệu in đậm, các kí hiệu kết thúc là các kí hiệu viết thường.

Start → **adjective noun tense verb**

adjective → the **size** / a **size**

size → tiny / small / large / big

noun → saw / ladder / truth / boy

tense → is / was

verb → waiting / standing

Kí hiệu chưa kết thúc đầu tiên là **adjective**. Luật cho kí hiệu chưa kết thúc này có hai sự lựa chọn tương đương (2^1) do đó một bit có thể được ẩn giấu bằng cách chọn một sự lựa chọn bên phải. Bit đầu tiên được giấu là 0, sự lựa chọn đầu tiên là (the **size**). Kí hiệu kết thúc “the” được nối vào văn bản còn kí hiệu chưa kết thúc **size** sẽ được thay thế tiếp. Từ **size** có bốn sự lựa chọn tương đương (2^2) nên có thể giấu được hai bit. Hai bit tiếp theo trong chuỗi cần giấu là bit 1 và bit 0, nên sự lựa chọn thứ ba, “large” sẽ được chọn. Kí hiệu chưa kết thúc tiếp theo là **noun**. Theo luật, có bốn sự lựa chọn nên có thể dùng hai bit tiếp theo trong chuỗi ẩn giấu. Ở đây, hai bit tiếp theo là bit 0 và bit 1 nên “ladder” được chọn. Sự lựa chọn cho **tense** là “was” (được chỉ ra bởi bit 1 tiếp theo), và sự lựa chọn cho **verb** là “waiting”, bởi vì bit cuối cùng là 0. Sau khi giấu tin thu được câu “the large ladder was waiting”. Câu này có thể gây nghi ngờ khi được đọc bởi một người bình thường nhưng nó lại dễ dàng vượt qua các kiểm tra của máy tính. Bộ mã hóa có thể dễ dàng kết thúc mỗi câu (tức là sau các lựa chọn của **verb**) với một dấu chấm câu và bắt đầu câu tiếp theo với một chữ cái viết hoa, để tăng tính thực tế cho các văn bản nhân tạo được sinh ra.

Thuật toán giấu tin:

Đầu vào:

- Thông điệp bí mật

- Bộ từ điển và các luật sinh

Các bước thực hiện:

- Bước 1: Chuyển đổi thông điệp bí mật sang dạng nhị phân
- Bước 2: Sinh chuỗi văn bản (G):
 - ✓ Nếu G rỗng: xuất “”
 - ✓ Nếu G là 1 ký tự kết thúc A: xuất “A”
 - ✓ Nếu G là 1 ký tự không kết thúc: với từng c trong luật sinh của G: bắt

đầu một sinh chuỗi (c) cho tới khi tất cả các luật sinh đều được duyệt

Đầu ra:

- Văn bản nhân tạo chứa thông điệp bí mật

Một CFG lớn với nhiều lựa chọn có thể ẩn nhiều bit hơn và tạo ra những câu có ý nghĩa tự nhiên hơn. Một CFG là không rõ ràng nếu một câu có thể được tạo ra bằng cách chọn những luật theo những thứ tự khác nhau. Điều này được thể hiện qua ví dụ sau

Start → **name action / who does**

name → Alice / Bob

action → is here / was there

who → Alice is / Bob was

does → here / there

Câu “Alice is here” có thể sinh ra bằng cách thay thế những kí hiệu không kết thúc **name action** bằng “Alice” và “is here”, đồng thời cũng có thể sinh ra bằng cách thay thế **who does** bằng “Alice is” và “here”. Hiển nhiên, một CFG sẽ tạo ra những văn bản có thể giải mã theo những cách khác nhau. CFG này là không phù hợp để ẩn giấu thông tin.

Một CFG ở dạng Greibach normal form (GNF) nếu kí hiệu chưa kết thúc luôn là sự lựa chọn cuối cùng trong các lựa chọn của luật sinh. Ví dụ, luật sinh có dạng **something** → A B | C D thuộc dạng GNF nhưng luật sinh dạng “**blah** → the **size** sum | a **size** bell” thì không thuộc dạng GNF. Tuy nhiên có thể sửa một luật không thuộc dạng GNF thành GNF bằng cách thêm các luật như sau:

adjective → the **sizesum** | a **sizebell**

sizesum → tiny sum | small sum | large sum | big sum

sizebell → tiny bell | small bell | large bell | big bell

Bộ giải mã sử dụng 1 CFG trong GNF để phân tích cú pháp, như trong ví dụ sau đây:

Start → **noun verb**

noun → Alice / Bob

verb → sent mail **to** / sent email **to**

to → to **rel recipient**

rel → all / some

recipient → friends / relatives

Để ẩn giấu chuỗi nhị phân 01010, bộ mã hóa chọn “Alice” cho bit đầu tiên (0) và “sent email **to**” cho bit thứ hai (1). Không từ nào có thể giấu thông tin khi luật thứ tư được áp dụng (bởi vì không có sự lựa chọn nào) nhưng bộ mã hóa sinh ra được kí hiệu kết thúc “to”, sau đó sử dụng luật sinh cho **rel** để chọn “all” cho bit thứ ba (0), và luật sinh cho **recipient** để chọn “relatives” cho bit thứ tư (1). Để ẩn bit thứ năm, bộ giải mã bắt đầu câu tiếp theo. Câu “Alice sent email to all relatives” có thể dễ dàng giải mã theo các thành phần cú pháp của câu và xác định được các bit ẩn.

Nhận xét: Ở ví dụ trên, chỉ có thể ẩn giấu được 4 bit trong câu “Alice sent email to all relatives” có độ dài 33 kí tự (bao gồm các khoảng trắng). Khả năng giấu tin trong ví dụ này chỉ là $4 / (33 * 8) \approx 0.015$ bit ẩn giấu trên mỗi bit của văn bản được tạo ra để giấu tin. Phương pháp này có thể tăng được tính hiệu quả nếu mỗi luật sinh có nhiều lựa chọn ở phần bên phải. Một luật sinh với 2^n sự lựa chọn có thể giấu được n bit. Nếu một lựa chọn là một từ có 4 chữ cái (tức là 32 bit) và có $1024 = 2^{10}$ lựa chọn trong luật sinh, thì 10 bit có thể ẩn giấu trong mỗi 32 bit của văn bản được sinh ra, dẫn đến khả năng giấu tin là $10 / 32 = 0.3125$ bits/bit (bpb). Phương pháp này đã được cài đặt và kiểm thử rộng rãi bởi tác giả Peter Wayner. So sánh với các thuật toán giấu tin khác, phương pháp này được đánh giá là đơn giản và có hiệu quả tốt.

5.3.2. Phương pháp dựa trên tính phản xạ đối xứng của ký tự

Trong hầu hết các thuật toán giấu tin, thông điệp bí mật được ẩn giấu bằng cách thay đổi cấu trúc của văn bản chứa do đó khả năng bị nghi ngờ hay mất mát dữ liệu khi gõ lại văn bản theo cấu trúc chính xác là có thể xảy ra. Để tránh xảy ra khả năng này cũng như tăng cường tính bảo mật, thay vì giấu các bit bí mật bằng cách thay đổi cấu trúc của văn bản chứa, phương pháp này sẽ giấu các thông điệp bí mật bằng cách tạo ra một văn bản tóm tắt thu thập từ các bài báo hay bất kỳ một phương tiện văn bản thông tin đại chúng. Quá trình tạo ra văn

bản tóm tắt phụ thuộc vào tính phản xạ đối xứng của bảng chữ cái tiếng Anh. Dựa vào tính chất này, bảng chữ cái được chia thành các bộ khác nhau, mỗi bộ đại diện cho một cặp bit. Để thực hiện điều này cần phân tích tính phản xạ đối xứng của bảng chữ cái tiếng Anh và phân loại chúng để thể hiện các bit. Các thuộc tính và các bit thể hiện tương ứng được trình bày như sau **Error! Reference source not found.**:

a) Phân loại bảng chữ cái tiếng Anh theo tính chất phản xạ đối xứng

Để phân loại bảng chữ cái tiếng Anh theo tính phản xạ đối xứng, đầu tiên chọn chiều ngang là trục đối xứng và phân chia các chữ cái tiếng Anh thành hai nhóm. Các chữ cái sau khi chia theo chiều ngang, nếu thu được hai phần giống hệt nhau, ví dụ chữ ‘B’, ‘H’,... xếp vào một nhóm, ngược lại, các chữ cái sau khi chia theo chiều ngang, nếu thu được hai phần không giống nhau, ví dụ chữ ‘A’, ‘F’,... xếp vào nhóm còn lại. Toàn bộ phân loại dựa trên logic này được trình bày trong bảng 5.1:

Bảng 5.1. Phân nhóm dựa trên tính phản xạ đối xứng theo trục ngang

ID nhóm	Tên nhóm	Chữ cái trong nhóm	Bit được gấu
1	Tính phản xạ đối xứng không được tuân thủ	A, F, G, J, L, M, N, P, Q, R, S, T, U, V, W, Y, Z	0
2	Tính phản xạ đối xứng được tuân thủ	B, C, D, E, H, I, K, O, X	1

Áp dụng tương tự với trục dọc, thu được hai nhóm như bảng 5.2:

Bảng 5.2. Phân nhóm dựa trên tính phản xạ đối xứng theo trục dọc

ID nhóm	Tên nhóm	Chữ cái trong nhóm	Bit được gấu
1	Tính phản xạ đối xứng không được tuân thủ	B, C, D, E, F, G, J, K, L, N, P, Q, R, S, Z	0
2	Tính phản xạ đối xứng được tuân thủ	A, H, I, M, O, T, U, V, W, X, Y	1

Kết hợp cả hai khái niệm được mô tả trong bảng 5.1 và bảng 5.2 có thể phân loại bảng chữ cái tiếng Anh thành bốn nhóm dựa trên cả hai chiều ngang và chiều dọc của chữ cái. Các chữ cái không đối xứng trên cả hai trục, ví dụ chữ ‘F’, chữ ‘G’,... được chia vào một nhóm. Các chữ cái đối xứng theo trục ngang, ví dụ chữ ‘B’, chữ ‘D’,... được chia vào một nhóm. Các chữ cái đối xứng theo trục dọc, ví dụ chữ ‘A’, chữ ‘M’ được chia vào một nhóm. Các chữ

cái đối xứng theo cả hai trục, ví dụ chữ ‘H’, chữ ‘I’ được chia vào một nhóm. Cụ thể, thu được bảng 5.3:

Bảng 5.3. Phân nhóm dựa trên tính phản xạ đối xứng theo trục ngang và trục dọc

ID nhóm	Tên nhóm	Chữ cái trong nhóm	Bit được giấu
1	Tính phản xạ đối xứng không được tuân thủ trên cả hai trục	F, G, J, L, N, P, Q, R, S, Z	00
2	Tính phản xạ đối xứng được tuân thủ trên trục ngang	B, C, D, E, K	01
3	Tính phản xạ đối xứng được tuân thủ trên trục dọc	A, M, T, U, V, W, Y	10
4	Tính phản xạ đối xứng được tuân thủ trên cả hai trục	H, I, O, X	11

b) Giấu tin trong văn bản sử dụng tính phản xạ đối xứng của bảng chữ cái tiếng Anh

Theo như sự phân loại bảng chữ cái tiếng Anh mô tả như trong bảng 5.3 dựa vào thông điệp bí mật và văn bản phủ được lựa chọn để sinh ra một văn bản tóm tắt có chứa thông điệp bí mật. Văn bản tóm tắt sẽ gồm các câu được trích ra từ văn bản lựa chọn. Các câu này sử dụng chữ cái đầu tiên của từ đầu tiên làm đại diện cho các cặp bit của thông điệp cần ẩn giấu.

Thuật toán giấu tin

Đầu vào:

- Thông điệp bí mật
- Bất kỳ văn bản bằng ngôn ngữ tiếng Anh

Các bước thực hiện:

- Bước 1: Biến đổi thông điệp bí mật thành chuỗi bit nhị phân
- Bước 2: Kiểm tra xem tổng độ dài của chuỗi bit là chẵn hay lẻ. Nếu lẻ, phải thêm 1 bit ‘0’ vào cuối chuỗi bit nhị phân. Bây giờ có thể chia chuỗi bit tổng thành các cặp bit liên tiếp.
- Bước 3: Chuyển đổi toàn bộ các ký tự của văn bản đầu vào thành các chữ cái viết hoa.
- Bước 4: Với từng cặp bit, xem xét chữ cái đầu tiên của từ đầu tiên trong câu:
 - ✓ Nếu chữ cái đó nằm trong nhóm đại diện cho cặp bit đang xem xét, chọn câu này và đưa vào văn bản chứa.
 - ✓ Nếu chữ cái đó không nằm trong nhóm đại diện cho cặp bit đang xem xét, bỏ qua câu này và chọn câu tiếp theo

- Bước 5: Quá trình tiếp diễn cho đến khi toàn bộ chuỗi bit của thông điệp bí mật được thực thi hết

- Bước 6: Văn bản mã hóa thu được là bản tóm tắt của văn bản đầu vào và được gửi đến người nhận

Đầu ra:

- Văn bản chứa thông điệp bí mật, hay chính là văn bản tóm lược của văn bản đầu vào

Thuật toán tách tin:

Đầu vào:

- Văn bản chứa thông điệp bí mật (đầu ra của thuật toán giấu tin)

Các bước thực hiện:

- Bước 1: Lấy các chữ cái đầu tiên của các từ đầu tiên trong từng câu.
- Bước 2: Dựa vào bảng 5.3 để lấy ra các cặp bit từ những chữ cái thu được và đưa ra một file.
- Bước 3: Chuyển đổi chuỗi bit nhị phân thành dạng chữ cái tương ứng.
- Bước 4: Toàn bộ thông điệp dưới dạng chữ cái thu được chính là thông điệp ẩn giấu

Đầu ra:

- Thông điệp bí mật

Ví dụ dưới đây sẽ làm rõ hơn về quy trình giấu tin sử dụng tính phản xạ đối xứng của bảng chữ cái tiếng Anh:

Thông điệp cần giấu là chuỗi bit “1100”.

Văn bản là vật chứa: “*Ostrich is a bird. Ostrich can fly. So many types of birds are there. Peacock is our national bird.*”.

Quá trình giấu: Để giấu hai bit đầu là 11, xem xét câu đầu tiên “*Ostrich is a bird.*”. Câu này bắt đầu bằng chữ cái ‘O’, thuộc nhóm 4, đại diện cho cặp bit 11 nên câu này được chọn. Tiếp theo, phải giấu cặp bit 00. Câu tiếp theo “*Ostrich can fly*” bắt đầu bằng chữ cái ‘O’, thuộc nhóm 4, đại diện cho cặp bit 11, nên bị bỏ qua. Tương tự, câu “*So many types of birds are there.*” bắt đầu bằng chữ cái ‘S’, thuộc nhóm 2, đại diện cho cặp bit 10, cũng bị bỏ

qua. Đến câu “*Peacock is our national bird.*” bắt đầu bằng chữ cái ‘P’, thuộc nhóm 1, đại diện cho cặp bit 00, sẽ được lựa chọn.

Văn bản chứa tin giấu là: “*Ostrich is a bird. Peacock is our national bird.*”

Nhận xét: Đây được coi là một phương pháp giấu tin an toàn, do không có bất kỳ thay đổi nào về mặt cấu trúc của nội dung văn bản và kẻ tấn công phải thực sự đọc chi tiết các câu của văn bản mới có thể nhận biết được văn bản này có gì bất thường hay không.

c) Giấu tin trong văn bản sử dụng tính phản xạ đối xứng của bảng chữ cái tiếng Việt

Phương pháp giấu tin dựa trên tính phản xạ đối xứng của ký tự có thể áp dụng cho việc giấu tin của các văn bản bằng tiếng Việt. Về bản chất, bảng chữ cái tiếng Việt cũng cùng hệ Latin với bảng chữ cái tiếng Anh, do đó có thể cải tiến phương pháp này để giấu tin cho văn bản tiếng Việt như sau:

- Không cần phải kiểm tra các mạo từ như “A”, “The” như trong phương pháp giấu thông tin bằng Tiếng Anh.

- Với thông điệp ẩn giấu, phải sử dụng bảng mã Unicode thay cho bảng mã ASCII. Tuy nhiên, để tối ưu hóa thông điệp ẩn giấu, sử dụng bảng mã ASCII để chuyển các ký tự thông dụng như các chữ cái trùng với bảng chữ cái tiếng Anh, chữ số, các dấu chấm câu,... Các ký tự này khi chuyển sang dạng chuỗi bit sẽ có độ dài là 1 byte (8-bit). Đối với các ký tự đặc biệt của riêng bảng chữ cái tiếng Việt (bao gồm cả chữ hoa, chữ thường và các dấu của tiếng Việt như huyền, sắc, hỏi, ngã, nặng), ví dụ như “Á”, “à”, “ê”, “đ”,... dùng phép mã hóa UTF-8 và với tùy ký tự sẽ thu được chuỗi bit có độ dài là 2 bytes (16-bit) hoặc 3 bytes (24-bits). Do các ký tự đặc biệt có độ dài lớn hơn các ký tự thuộc bảng mã ASCII nên văn bản dùng để chứa thông điệp ẩn giấu sẽ có kích thước lớn hơn.

- Với hệ thống bản đồ để mã hóa các cặp bit, phải thêm các chữ cái tiếng Việt, ví dụ như “Á”, “À”, “Ã”, “Â”, “Đ”, “Ê”, “Ô”, “U”,... và phải bỏ các chữ cái “F”, “J”,.. của bảng chữ cái tiếng Anh... Chi tiết bản đồ mã hóa các ký tự thành các cặp bit như sau:

Bảng 5.4. Mã hóa các ký tự Tiếng Việt thành cặp bit

và thông tin có thể được ẩn giấu dựa vào cú pháp thay đổi này. Phương pháp này giấu được ít thông tin và có hiệu suất thấp vì phải có sự điều chỉnh thủ công. Tuy nhiên phương pháp này an toàn vì rất khó để máy tính có thể phát hiện ra sự thay đổi cú pháp giữa hai cụm từ. Kẻ tấn công phải thực sự đọc các tin nhắn một cách thủ công và xác định những cụm từ có liên quan để trích xuất dữ liệu.

5.4.2. Phương pháp sử dụng ngữ nghĩa

Phương pháp sử dụng ngữ nghĩa là phương pháp mà dữ liệu được giấu trong văn bản bằng cách sử dụng các từ đồng nghĩa. Ở phương pháp này thì người gửi và người nhận sẽ sử dụng cùng một bộ từ điển trực tuyến nhất định. Đây có thể coi là một tập dữ liệu chứa những từ quy ước và bộ giải mã sẽ đọc từng từ trong văn bản và tìm kiếm những từ tương ứng trong từ điển [29].

a) Sử dụng từ đồng nghĩa

Các bộ giải mã đọc từng từ trong văn bản và tìm kiếm từ đồng nghĩa trong từ điển, nếu một từ chẳng hạn như “god child”, không có từ đồng nghĩa nào thì các bộ giải mã giả định rằng không có dữ liệu nào được giấu trong đó. Nếu từ “child” là đầu vào, và chính nó xuất hiện trong từ điển như một từ đồng nghĩa trong danh sách (bud, chick, child, kid, minor), sau đó, danh sách này sẽ được xem như là để che giấu hai bit và “child” (là từ thứ 3 trong danh sách) được hiểu là ẩn giấu số 2 bit 2 (01 trong hệ nhị phân).

Thuật toán giấu tin:

Đầu vào:

- Thông điệp bí mật
- Văn bản phủ

Các bước thực hiện:

- Bước 1: Chuyển thông tin mật thành dạng nhị phân.
- Bước 2: Kiểm tra văn bản và chọn một từ xuất hiện nhiều lần
- Bước 3: Sử dụng từ điển đặc biệt chọn những từ đồng nghĩa để thay cho từ được chọn theo quy ước và chuỗi nhị phân.

Đầu ra:

- Văn bản phủ có chứa thông điệp.

b) Trích rút câu

Một hướng tiếp cận khác của phương pháp giấu tin bằng ngữ nghĩa là định nghĩa một hàm rút một câu thành một bit dữ liệu. Cách làm ở đây có thể là kiểm tra tính chẵn lẻ của mã ASCII trong tất cả các ký tự ở trong câu. Trong một ứng dụng thực tế của phương pháp này, bộ xử lý văn bản đã được chỉnh sửa như sau:

- Đầu tiên, bộ xử lý văn bản nhận thông tin cần giấu và chứa chúng trong một chuỗi bit.
- Bộ xử lý văn bản nhận những ký tự của văn bản thường được nhập vào theo chu kỳ, đưa vào hàm xử lý và so sánh kết quả của nó với bit thông tin được ẩn giấu tiếp theo.
- Nếu tính chẵn lẻ của tất cả các mã ASCII của câu hiện tại có một bit lệch với bit của chuỗi bit cần giấu thông tin, bộ xử lý văn bản sẽ từ chối không cho gõ thêm các ký tự khác. Lựa chọn duy nhất là người dùng sẽ phải viết lại câu.

5.5. Phương pháp phát hiện giấu tin trong văn bản

Các phương pháp phát hiện thông tin được giấu trong văn bản hiện nay đều dựa vào đặc điểm của các phương pháp giấu tin trong văn bản. Do đặc điểm của các kỹ thuật giấu tin trong văn bản nên mỗi phương pháp giấu tin đều có những nhược điểm nhất định. Chính vì vậy trong thực tế, để phát hiện giấu tin trong văn bản những người phân tích thường áp dụng một số phương pháp sau [1, 2, 31]:

- Phát hiện giấu tin dựa vào khoảng trắng: Trong văn bản, những thay đổi nhỏ trong từ và khoảng cách dòng có thể khó phát hiện bởi người quan sát bình thường. Tuy nhiên, các khoảng trống phụ và các ký tự "vô hình" có thể dễ dàng được tiết lộ bằng cách mở tệp tin bằng một trình xử lý văn bản thông dụng. Văn bản có thể trông "bình thường" nếu được gõ trên màn hình, nhưng nếu tệp được mở trong trình xử lý văn bản, dấu cách, các tab và các ký tự khác làm biến dạng bản trình bày của văn bản

- Phát hiện giấu tin dựa vào cú pháp và ngữ nghĩa: Với giấu tin ngữ nghĩa cần có hiểu biết về câu từ trong đoạn văn, nghĩa của loại văn bản đó, với loại giấu tin này cần phát hiện các đoạn viết không được mượt, các đoạn vô nghĩa, từ đồng nghĩa, các lỗi chính tả cố tình. Về phần phát hiện giấu tin này thì dựa vào hoàn toàn vào khả năng hiểu biết về văn bản của người kiểm tra.

- Phương pháp phát hiện dựa trên phân tích các tính năng thống kê sử dụng học máy: Phương pháp này ban đầu sẽ nghiên cứu các mô hình thống kê của các văn bản tự nhiên, và chỉ ra rằng giấu thông tin trong văn bản có thể thay đổi các tính năng của văn bản bằng cách

phân tích các tính năng thống kê. Văn bản tự nhiên và văn bản có giấu tin có các tính năng khác nhau như sau [31]:

✓ Chiều dài trung bình của từ: Theo nguyên tắc của Zipf và Heaps, độ dài trung bình của từ nằm trong phạm vi nhất định. Văn bản được giấu tin là khi các thông tin mật được giấu vào văn bản, sự lựa chọn của các từ rất ngẫu nhiên, vì vậy có ít từ tần số cao hơn trong văn bản thông thường và chiều dài trung bình của từ dài hơn. Để tăng sự che giấu văn bản và giảm mức trung bình chiều dài của từ thì công cụ giấu tin sẽ làm tăng số lượng từ ngắn khi tạo văn bản giấu tin.

✓ Tỷ lệ khoảng trắng: Theo nguyên tắc Heap, tỷ lệ khoảng trắng của văn bản xấp xỉ tỷ lệ nghịch với chiều dài từ và dấu chấm câu không được tính. Nếu khoảng trắng xuất hiện hai lần hoặc nhiều hơn thì có thể có cơ sở để kết luận văn bản đó bất thường. Rõ ràng, việc phát hiện này làm nâng cao hiệu quả trong việc xác định văn bản chứa thông tin mật sử dụng các thuật toán ẩn thay giấu tin đổi số khoảng trắng trong văn bản.

✓ *N* từ đầu tiên và từ không hợp lệ: Theo lý thuyết TF-IDF, các từ có tần số cao bao gồm các từ tần số cao hiệu quả (AFW) và các từ tần số cao không hợp lệ (NFW). AFW là một từ khóa hợp lệ để thể hiện chủ đề của một bài viết, trong khi NFW là các từ không có ý nghĩa, chẳng hạn như "the", "of", v.v.

✓ Phần trăm của chữ cái: Trong các bài báo tiếng Anh, khi số lượng văn bản nhỏ, việc phân phối các chữ cái văn bản sẽ thay đổi rất nhiều. Như số lượng văn bản tăng lên, tính ngẫu nhiên của các chữ cái tăng, và phần trăm chữ cái là gần như không thay đổi.

✓ Phần trăm chữ cái đầu: Việc phân phối các chữ cái ban đầu của văn bản tiếng Anh có liên quan đến việc phân phối các chữ cái ban đầu của một từ điển. Vì sự phân bố của các chữ cái ban đầu trong từ điển rất khác nhau dẫn đến sự phân bố ban đầu của văn bản rất khác nhau. Tính ngẫu nhiên của các văn bản chứa tin mật và văn bản tự nhiên sẽ khác nhau.

Dựa vào năm trích chọn đặc trưng (thuộc tính) có thể áp dụng vào thuật toán học máy để phát hiện văn bản có chứa tin mật.

5.6. Câu hỏi ôn tập

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

Câu 2. Hãy trình bày các phương pháp phân loại giấu tin trong văn bản?

- Câu 3. Hãy trình bày quy trình giấu tin trong văn bản sử dụng phương pháp khoảng trắng giữa các từ
- Câu 4. Hãy trình bày quy trình giấu tin trong văn bản sử dụng phương pháp dịch chuyển dòng?
- Câu 5. Hãy trình bày quy trình giấu tin trong văn bản sử dụng phương pháp dịch chuyển vị trí từ?
- Câu 6. Hãy trình bày quy trình giấu tin tính phản xạ đối xứng của bảng chữ cái tiếng Anh?
- Câu 7. Hãy trình bày quy trình giấu tin trong văn bản sử dụng phương pháp cú pháp?
- Câu 8. Hãy trình bày quy trình giấu tin trong văn bản sử dụng phương pháp từ đồng nghĩa?
- Câu 9. Hãy trình bày quy trình giấu tin trong văn bản sử dụng phương pháp trích rút câu?
- Câu 10. Hãy trình bày phương pháp phát hiện giấu tin trong văn bản sử dụng kỹ thuật học máy?
- Câu 11. Hãy trình bày quy trình giấu tin trong văn bản sử dụng tính phản xạ đối xứng của bảng chữ cái tiếng Việt?
- Câu 12. Hãy trình bày quy trình giấu tin trong văn bản sử dụng văn phạm phi ngữ cảnh?

TÀI LIỆU THAM KHẢO

- [1] Konakhovich Georgiy Filimonovich; Puzyrenko Alexander Yurievich. Computer Steganography. Theory and practice. "MK-Press", 2006; 288p.
- [2] Fabien A. Petitcolas, Stefan Katzenbeisser. Information Hiding Techniques for Steganography and Digital Watermarking. Boston, London: Artech House, 1999.
- [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. Advances in Cryptology — EUROCRYPT '96 pp 84-95.
- [5] Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton Kalker, Digital Watermarking and Steganography. Series Editor. Morgan Kaufmann Publishers is an imprint of Elsevier. 30 Corporate Drive, Suite 400, Burlington, MA 01803, USA
- [6] Microsoft Windows Bitmap File Format Summary. <https://www.prepressure.com/library/file-formats/bmp>. [Ngày truy cập 22/5/2018].
- [7] PNG (Portable Network Graphics) Specification, Version 1.2. <http://www.libpng.org/pub/png/spec/1.2/PNG-Structure.html>. [Ngày truy cập 22/5/2018].
- [8] JPEG File Interchange Format File Format Summary. <https://www.fileformat.info/format/jpeg/egff.htm>. [Ngày truy cập 22/5/2018].
- [9] ITU (1993), Information technology – digital compression and coding of continuous-tone still images – requirements and guidelines (ISO/IEC 10918-1: 1993(E)).
- [10] Shih, Frank Y. Digital Watermarking and Steganography: Fundamentals and Techniques (Second Edition). Taylor & Francis, CRC Press, 2017.
- [11] Unik Lokhande. A. K. Gulve Steganography using Cryptography and Pseudo Random Numbers. International Journal of Computer Applications (0975 – 8887) Volume 96– No.19, June 2014.
- [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 3796 (2005) 355{375. Springer-Verlag.

- [13]Po-Yueh Chen and Hung-Ju Lin, “A DWT Based Approach for Image Steganography”, International Journal of Applied Science and Engineering 4, 3: 275-290, 2006.
- [14]Chun-Shien Lu, Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property, IDEA Group Publishing, 2005
- [15]Vijay Kumar, Dinesh Kumar. A modified DWT-based image steganography technique. Multimedia Tools and Applications An International Journal. Springer Science+Business Media, LLC 2017.
- [16]Sheelu (M. Tech (CSE) - Manav Rachna College Of Engineering, Faridabad, India) “Enhancement of Data Hiding Capacity in Audio Steganography”, IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 13, Issue 3 Jul. - Aug. 2013
- [17]Pradeep Kumar Singh, R.K.Aggrawal: Enhancement of LSB based Steganography for Hiding Image in Audio, (IJCSSE) International Journal on Computer Science and Engineering Vol. 02, No. 05, 2010, 1652-1658.
- [18]B.C..J Moore: An introduction to the Psychology of Hearing, Academic Press. 2001
- [19]Đỗ Quốc Trinh, Vũ Thanh Hải: Kỹ thuật trải phổ và ứng dụng. Học viện kỹ thuật quân sự 2006.
- [20]L. Boney, A. H. Tewfik and K. N. Hamdy, “ Digital Watermarks for Audio signals” IEEE int. conf. On multimedia Computing and System, Horoshima, Japan, June 1996.
- [21]I.J.COX, “ Spread Spectrue Watermark for Embedded Signaling” United states Patent 5,848,155, December 1988 Dec.
- [22]Cox I, Miller M & McKellips A (1999) Watermarking as communications with side information. Proceedings of he IEEE 87.
- [23]Malvar H & Florencio D (2003) Improved spread spectrum: Anew modulation technique for robust watermarking.
- [24]Gerrit Cornelis LANGELAAR (2000). Real-time Watermarking Techniques for Compressed Video Data. Veenendaal ISBN 90-9013190-6.
- [25]Tìm hiểu về các định dạng file video phổ biến. <https://quantrimang.com/tim-hieu-ve-cac-dinh-dang-file-video-42612>. [Ngày truy cập 30/8/2018].
- [26]Video Steganography based on Scene Change Detection – 1 J.Mary Jenifer, 2 Dr.S.Raja Ratna PG Scholar, Associate Professor Computer Science and Engineering VV College of Engineering, Tuticorin, India.
- [27]Shuliang Sun. A New Information Hiding Method Based on Improved BPCS Steganography. Advances in Multimedia Volume 2015, Article ID 698492, 7 p.

- [28]David Salomon. Data Privacy and Security. Springer, Verlag, 2003.
- [29]Anandaprova Majumder, Suvamoy Changder. A Novel Approach for Text Steganography: Generating Text Summary using Reflection Symmetry. International Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA) 2013.
- [30]W. Bender, D. Gruhl, N. Morimoto, A. Lu. Techniques for data hiding. IBM Systems Journal, Volume: 35 Issue: 3&4.
- [31]Chen Zhi-li, Huang Liu-sheng, Yu Zhen-shan, Zhao Xin-xin, Zheng Xue-ling, Effective Linguistic Steganography Detection, Department of Computer Science and Technology, University of Science and Technology of China, National High Performance Computing Center(Hefei), Hefei, Anhui 230027, China.
- [32] Natarajan Meghanathan, Lopamudra Nayak. A Review of the Audio and Video Steganalysis Algorithms. Proceedings of the 48th Annual Southeast Regional Conference, 2010, Oxford, MS, USA, April 15-17, 2010.