**BAN CƠ YẾU CHÍNH PHỦ**

**HỌC VIỆN KỸ THUẬT MẬT MÃ**

**---🙠**🕮**🙢---**



**KỸ THUẬT GIẤU TIN**

**ẨN MÃ TRONG ẢNH SỬ DỤNG PHƯƠNG PHÁP PVD VÀ QRT**

Ngành: An toàn thông tin

Mã số: 7.48.02.02

*Sinh viên thực hiện***:**

**Nguyễn Đức Thịnh – AT160446**

**Nguyễn Tài Phúc – AT160437**

**Lưu Văn Tùng – AT160456**

*Người hướng dẫn:*

TS. Trần Thị Xuyên

Hà Nội, 2023

**MỤC LỤC**

[**LỜI NÓI ĐẦU 2**](#_Toc127869840)

[**CHƯƠNG 1. TỔNG QUAN VỀ KỸ THUẬT GIẤU TIN 3**](#_Toc127869841)

[**1.1. Giới thiệu về Steganography 3**](#_Toc127869842)

[**1.2. Các khái niệm cơ bản trong Steganography 5**](#_Toc127869843)

[**1.3. Steganography trong an toàn thông tin hiện nay 8**](#_Toc127869844)

[**1.3.1. Phân loại Steganography trong an toàn thông tin 9**](#_Toc127869845)

[**a. Giấu tin trong video 10**](#_Toc127869846)

[**b. Giấu tin trong audio 11**](#_Toc127869847)

[**c. Giấu tin trong ảnh 11**](#_Toc127869848)

[**d. Giấu tin trong văn bản 12**](#_Toc127869849)

[**1.3.2. Giới thiệu một số kỹ thuật giấu tin 12**](#_Toc127869850)

[**a. Kỹ thuật giấu tin LSB 12**](#_Toc127869851)

[**b. Kỹ thuật giấu tin trên miền biến đổi tần số DCT 14**](#_Toc127869852)

[**c. Phương pháp Pixel Value Difference (PVD) 15**](#_Toc127869853)

[**d. Phương pháp Quantized Range Table (QRT) 15**](#_Toc127869854)

[**1.3.3. Tầm quan trọng của Steganography trong an toàn thông tin 16**](#_Toc127869855)

[**CHƯƠNG 2. ẨN MÃ TRONG ẢNH SỬ DỤNG PHƯƠNG PHÁP PVD VÀ QRT 19**](#_Toc127869856)

[**2.1. Phương pháp PVD 19**](#_Toc127869857)

[**2.1.1. Lượng tử hóa sự khác biệt các giá trị màu xám của khối hai điểm ảnh 20**](#_Toc127869858)

[**2.1.2. Quá trình nhúng dữ liệu 22**](#_Toc127869859)

[**2.1.3. Quá trình trích xuất thông tin từ ảnh stegano 24**](#_Toc127869860)

[**2.2. Phương pháp QRT 26**](#_Toc127869861)

[**2.2.1. Kĩ thuật nhúng 27**](#_Toc127869862)

[**2.2.2. Kĩ thuật trích xuất 28**](#_Toc127869863)

[**2.2.3. Ưu, nhược điểm 29**](#_Toc127869864)

[**CHƯƠNG 3. THỰC NGHIỆM 31**](#_Toc127869865)

[**3.1. Kết quả thực nghiệm phương pháp PVD 31**](#_Toc127869866)

[**KẾT LUẬN 36**](#_Toc127869867)

[**TÀI LIỆU THAM KHẢO 37**](#_Toc127869868)

# LỜI NÓI ĐẦU

Cuộc cách mạng thông tin kỹ thuật số đã đem lại những thay đổi sâu sắc trong xã hội và trong cuộc sống của chúng ta. Những thuận lợi mà thông tin kỹ thuật số mang lại cũng sinh ra những thách thức và cơ hội mới cho quá trình phát triển. Internet và mạng không dây đã trợ giúp cho việc chuyển phát một khối lượng thông tin rất lớn qua mạng. Tuy nhiên nó cũng làm tăng nguy cơ sử dụng trái phép, xuyên tạc bất hợp pháp các thông tin được lưu chuyển trên mạng, đồng thời việc sử dụng một cách bình đẳng và an toàn các dữ liệu đa phương tiện cũng như cung cấp một cách kịp thời tới rất nhiều người dùng cuối và các thiết bị cuối cũng là một vấn đề quan trọng và còn nhiều thách thức. Hơn nữa sự phát triển của các phương tiện kỹ thuật số đã làm cho việc lưu trữ, sửa đổi và sao chép dữ liệu ngày càng đơn giản, từ đó việc bảo vệ bản quyền và chống xâm phạm trái phép các dữ liệu đa phương tiện (âm thanh, hình ảnh, tài liệu) cũng gặp nhiều khó khăn.

Một hình thức mới được ra đời đã phần nào giải quyết được các khó khăn trên đó là giấu thông tin trong các nguồn đa phương tiện như các nguồn âm thanh, hình ảnh, ảnh tĩnh...Xét theo khía cạnh tổng quát thì giấu thông tin cũng là một hệ mật mã nhằm đảm bảo tính an toàn thông tin, những phương pháp này ưu điểm ở chỗ giảm được khả năng phát hiện ra sự tồn tại của thông tin trong các nguồn mạng. Không giống như mã hoá thông tin là để chống sự truy cập và sửa chữa một cách trái phép thông tin. Giấu và phát hiện thông tin là kỹ thuật còn tương đối mới và đang phát triển rất nhanh thu hút được sự quan tâm của cả giới kểóa học và giới công nghiệp nhưng cũng còn rất nhiều thách thức. Tuy nhiên làm thế nào để tiến hành thực hiện được việc giấu thông tin một cách an toàn, thông tin không bị phát hiện?

Để tìm hiểu sâu hơn về công nghệ giấu tin, các phương ẩn giấu mật mã cũng như cách thực hiện công nghệ này, chúng em đã lựa chọn đề tài “Ẩn mã trong ảnh sử dụng phương pháp PVD và QRT”.

Tài liệu này bao gồm 3 phần chính:

Chương 1: Tổng quan về STEGANOGRAPHY

Chương 2: Ẩn mã trong ảnh sử dụng phương pháp PVD và QRT

Chương 3: Thực nghiệm

# TỔNG QUAN VỀ KỸ THUẬT GIẤU TIN

## Giới thiệu về Steganography

Steganography (kỹ thuật giấu tin) là kỹ thuật che giấu một tập tin, thông điệp, hình ảnh hoặc video trong các tập tin, thông điệp, hình ảnh hoặc video khác. Thuật ngữ Steganography được hình thành nhờ sự kết hợp của những từ Hi Lạp là: Steganos, có nghĩa là “bao phủ, che dấu hoặc bảo vệ” và Graphein, có nghĩa là “viết”.

Các ghi nhận đầu tiên về thuật ngữ này do Johannes Trithemius sử dụng trong cuốn sách Steganographia của ông vào năm 1499, một luận thuyết về mật mã và giấu tin được ngụy trang như một cuốn sách ma thuật. Các thông điệp bí mật được ẩn hoặc trở thành một phần của một đối tượng hoàn toàn khác như: Hình ảnh, bài viết, danh sách hoặc một số dạng văn bản che giấu khác.

Yêu cầu quan trọng nhất của bất kỳ hệ thống Steganography nào là con người hoặc máy tính không thể phân biệt một cách dễ dàng giữa các đối tượng bình thường và đối tượng có chứa dữ liệu bí mật.

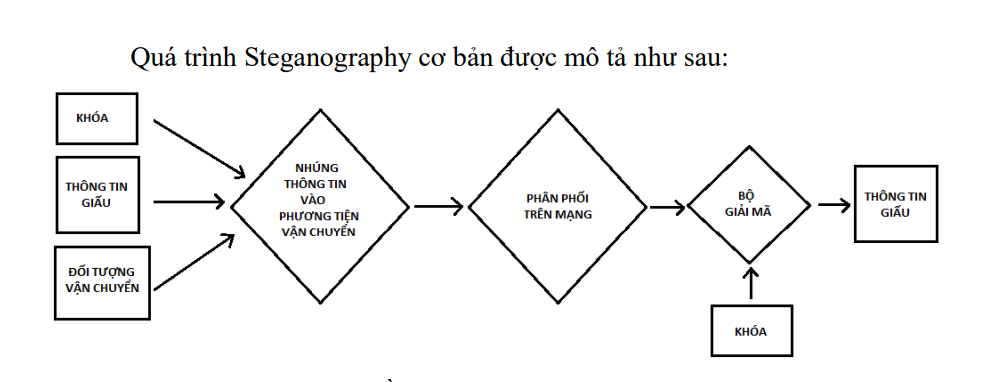
Steganography bao gồm cả việc che giấu thông tin trong các tập tin máy tính. Trong lĩnh vực giấu tin kỹ thuật số, các thông tin liên lạc điện có thể bao gồm giấu tin mã hóa bên trong tầng vận chuyển, chẳng hạn như một tập tin tài liệu, tập tin ảnh, phần mềm hoặc giao thức. Các tập tin đa phương tiện rất phù hợp cho việc truyền giấu tin bởi vì chúng có kích thước tập tin lớn.

Steganography gồm 2 thành phần chính:

- Thuật toán giấu tin.

- Bộ giải mã thông tin.

Thuật toán giấu tin được dùng để giấu thông tin vào một đối tượng vận chuyển bằng cách sử dụng một khóa bí mật được dùng chung bởi người mã hóa và người giải mã, việc giải mã thông tin chỉ có thể thực hiện được khi có khoá. Bộ giải mã thực hiện giải mã trên đối tượng vận chuyển đã chứa dữ liệu để trả lại thông điệp ẩn trong nó.



Hình 1.1. Lược đồ chung cho quá trình Steganography

Trong đó:

- Đối tượng vận chuyển bao gồm các đối tượng được dùng làm môi trường để giấu tin như: Text, audio, video, ảnh,…

- Giấu thông tin là mục đích của người sử dụng, thông tin giấu là một lượng thông tin mang một ý nghĩa nào đó như ảnh, logo, đoạn văn bản… tùy thuộc vào mục đích của người sử dụng.

- Thông tin sẽ được giấu vào trong đối tượng vận chuyển nhờ một bộ nhúng, bộ nhúng là những phần mềm, triển khai các thuật toán để giấu tin và được thực hiện với một khóa bí mật giống như các hệ mã cổ điển.

- Sau khi giấu tin ta thu được đối tượng vận chuyển chứa thông tin bí mật và được phân phối sử dụng trên mạng.

- Sau khi nhận được đối tượng vận chuyển có giấu thông tin, quá trình giải mã được thực hiện thông qua một bộ giải mã tương ứng với bộ nhúng thông tin cùng với khóa của quá trình nhúng.

- Kết quả thu được gồm đối tượng vận chuyển ban đầu và thông tin đã giấu. Cuối cùng thông tin giấu sẽ được xử lý kiểm định để xác nhận nguồn gốc của thông tin.

Mục đích chính của Steganography là giấu đi những thông điệp bí mật khỏi việc kiểm duyệt, gián điệp hay kẻ trộm. Những thông điệp tưởng chừng như vô hại và nhàm chán cũng có thể thu hút sự chú ý.

Những thông điệp đã được mã hóa có thể sẽ không bị giải mã và phát hiện bởi những thế lực thù địch, nhưng việc sử dụng mã hóa có thể làm kẻ địch tin rằng thông tin có chứa thông tin nhạy cảm hoặc không hợp pháp dù nó có hay không. Ở một số nơi, việc sử dụng mức độ bảo mật cao có thể bị hạn chế hoặc bị cấm. Steganography cho phép thông điệp đã mã hóa được ẩn đi và tránh khỏi những sự tò mò của người khác.

Trong khi Cryptography (mật mã học) chỉ là việc bảo vệ các nội dung của một thông điệp đơn thuần, Steganography còn liên quan với việc che giấu sự thật trong quá trình truyền gửi một thông điệp bí mật, cũng như che giấu nội dung của thông điệp.

Ưu điểm của Steganography là những thông điệp bí mật được chủ ý không để thu hút sự chú ý đến bản thân nó. Rõ ràng ta có thể nhìn thấy các thông điệp đã được mã hóa, tránh được sự tò mò, quan tâm của những người khác. Steganography làm rất tốt trong việc giấu đi 1 lượng nhỏ dữ liệu bí mật.

Hạn chế lớn nhất của Steganography là các tập tin vận chuyển phải lớn hơn đáng kể so với những dữ liệu đã được ẩn. Ví dụ, ta không thể ẩn nội dung của một cuốn sách lớn trong một tệp hình ảnh nhỏ.

## Các khái niệm cơ bản trong Steganography

Để hiểu rõ hơn về Steganography cũng như dễ dàng tìm hiểu hiểu các nội dung trong các phần tới, phần này sẽ đề cập đến một số khái niệm cần chú ý trong lĩnh vực Steganography:

* Giấu tin: Là quá trình ẩn một dữ liệu vào trong một môi trường dữ liệu khác. Dữ liệu trước khi giấu có thể được nén và mã hoá bằng nhiều cách.

Trong các ứng dụng đòi hỏi độ bảo mật cao, việc giấu dữ liệu chính là một phương pháp bảo mật thông tin hiệu quả. Việc giấu dữ liệu được ứng dụng trong nhiều lĩnh vực khác nhau như bảo vệ bản quyền, ngăn ngừa sao chép trái phép, truyền thông bí mật v.v..

* Giấu tin trong dữ liệu đa phương tiện: Là một phần của khái niệm “giấu tin” với việc sử dụng dữ liệu đa phương tiện làm phương tiện vận chuyển.

Giấu thông tin trong dữ liệu đa phương tiện có nhiều ứng dụng trong thực tế như trong việc xác định quyền sở hữu, chống xuyên tạc thông tin và chuyển giao dữ liệu một cách an toàn.

* Secret Messages (thông điệp bí mật): Là các thông tin, dữ liệu quan trọng mà chúng ta cần che dấu, đảm bảo bí mật và cần được bảo vệ trong quá trình truyền tải.
* Carrier (đối tượng vận chuyển): Là tín hiệu, luồng hoặc tệp dữ liệu mà trong đó dữ liệu ẩn được che dấu bằng những cách sửa đổi tinh vi. Ví dụ như: Tập tin âm thanh, hình ảnh, tài liệu, v.v..

Một số thuộc tính dẫn đến việc nghi ngờ một tệp tin đang chứa dữ liệu ẩn:

+ Nếu dữ liệu ẩn có kích thước lớn so với nội dung của nhà cung cấp, như kích thước 1 megabyte trong một tập tin tài liệu trống.

+ Việc sử dụng các định dạng đã lỗi thời hoặc phần mở rộng được hỗ trợ kém.

Một yêu cầu mật mã là các Carrier phải là bản gốc, không phải bản sao của một thứ gì đã được công khai, ví dụ như đã được tải lên Internet. Vì mã nguồn dữ liệu công khai có thể được đối chiếu với phiên bản có chứa một thông điệp ẩn đã được nhúng vào.

Một yêu cầu nữa là thông điệp được nhúng không thay đổi số liệu thống kê của một Carrier (hoặc các chỉ số khác) vì sự hiện diện của một thông điệp có thể bị phát hiện.

* Carrier Engine: Là lõi của bất cứ một công cụ Steganography nào.

Các định dạng tệp khác nhau được sửa đổi theo nhiều cách khác nhau để dữ liệu ẩn được ẩn bên trong chúng. Các thuật toán xử lý bao gồm:

+ Injection

+ Generation

+ Dữ liệu phụ (Ancillary data) và thay thế siêu dữ liệu (Metadata Substitution).

+ LSB (Least Significant Bit) hoặc thay thế thích ứng (adaptive substitution).

+ Thao tác không gian tần số (Frequency space manipulation).

* Carrier Chain (chuỗi đối tượng vận chuyển): Dữ liệu ẩn có thể được phân chia giữa một tập hợp các tập tin, tạo ra một Carrier Chain, trong đó có các tính chất mà tất cả các đối tượng vận chuyển phải có là: Tính khả dụng, tính toàn vẹn và phải được xử lý theo thứ tự chính xác để lấy các dữ liệu ẩn.

Tính năng bảo mật bổ sung này thường đạt được bằng cách:

+ Sử dụng Vector khởi tạo khác nhau cho mỗi đối tượng vận chuyển và lưu trữ nó bên trong các đối tượng vận chuyển đã được xử lý, điều này có nghĩa là: CryptedIVn = Crypt (IVn, CryptedIVn-1).

+ Sử dụng một thuật toán mật mã khác cho mỗi đối tượng vận chuyển và lựa chọn nó bằng một thuật toán chuỗi thứ tự phụ thuộc.

* Modified Carrier (ModCarrier): Là các đối tượng vận chuyển sau khi đã được sửa đổi, cũng có nghĩa là chúng đã được nhúng các thông điệp bí mật.
* Embedded (nhúng): Cách viết khác Embedding, Imbedded hoặc Imbedding, là quá trình nhúng các thông điệp bí mật vào trong một dữ liệu môi trường nào đó, ví dụ như các tập tin vận chuyển.
* Obfuscation (sự xáo trộn): Là cố ý che dấu về ý nghĩa có dụng ý của truyền thông, thường bằng cách làm cho thông điệp trở nên dễ nhầm lẫn, mơ hồ hoặc khó hiểu.
* Noise (nhiễu): Là sự xuất hiện những đặc điểm lạ của thông điệp bí mật cần được nhúng so với lúc ban đầu. Việc này nhằm mục đích là thông điệp bí mật trở nên khó hiểu để được bảo mật cao hơn.
* Digital Watermark (thủy vân số): Là một loại đánh dấu bí mật được dấu trong một tín hiệu chứa nhiễu như dữ liệu âm thanh, hình ảnh hoặc video. Nó thường được sử dụng để xác định quyền sở hữu bản quyền của tính hiệu đó. Digital Watermark là quá trình giấu thông tin kỹ thuật số trong một tín hiệu Carrier, nhưng không cần có một mối quan hệ với các tính hiệu Carrier đó.

Digital Watermark có thể được sử dụng để xác minh tính xác thực hoặc tính toàn vẹn của tín hiệu Carrier hoặc để hiển thị danh tính của chủ sở hữu. Nó được sử dụng rộng rãi để theo dõi vi phạm bản quyền và để xác thực tiền giấy. Giống như các Physical Watermark, Digital Watermark thường chỉ nhận biết được trong điều kiện nhất định, ví dụ như sau khi sử dụng một số thuật toán. Nếu một Digital Watermark làm thay đổi tín hiệu Carrier theo cách mà nó trở nên dễ nhận thấy, nó có thể được coi là kém hiệu quả tùy thuộc vào mục đích sử dụng của nó. Các Watermark truyền thống có thể được áp dụng cho các dữ liệu đa phương tiện có thể nhìn thấy, giống như hình ảnh hoặc video, trong khi ở Digital Watermarking, tín hiệu có thể là âm thanh, hình ảnh, video, văn bản hoặc mô hình 3D. Một tín hiệu có thể mang nhiều Watermark khác nhau cùng một lúc. Không giống như siêu dữ liệu được thêm vào tín hiệu Carrier, một Digital Watermark không thay đổi kích thước của tín hiệu Carrier.

Các thuộc tính cần thiết của một Digital Watermark phụ thuộc vào các trường hợp sử dụng nơi mà nó được áp dụng. Để đánh dấu các tệp phương tiện với thông tin bản quyền, một Digital Watermark phải tương đối mạnh mẽ chống lại những sửa đổi có thể được áp dụng cho tín hiệu Carrier. Thay vào đó, nếu đảm bảo tính toàn vẹn, một Watermark dễ gãy vỡ sẽ được áp dụng. Cả Steganography và Digital Watermark đều sử dụng các kỹ thuật Steganographic để nhúng dữ liệu bí mật trong tín hiệu nhiễu. Tuy nhiên, trong khi Steganography nhằm mục đích không nhận thấy đối với các giác quan của con người, Digital Watermarking cố gắng kiểm soát tính mạnh mẽ như là ưu tiên hàng đầu. Digital Watermark là một công cụ bảo mật thụ động. Nó chỉ đánh dấu dữ liệu chứ không làm suy giảm nó hoặc kiểm soát truy cập vào dữ liệu.

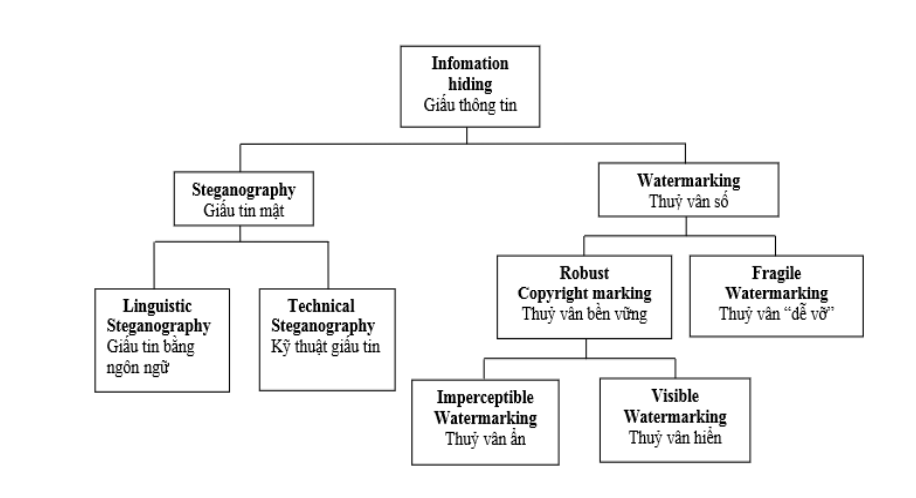
* Tính không nhìn thấy: Là một trong ba yêu cầu của bất kỳ một hệ giấu tin nào.Tính không nhìn thấy là tính chất vô hình của thông tin nhúng trong phương tiện nhúng.
* Tính mạnh mẽ: Là yêu cầu thứ hai của một hệ giấu tin. Tính mạnh mẽ là nói đến khả năng chịu được các thao tác biến đổi nào đó trên phương tiện nhúng và các cuộc tấn công có chủ đích.
* Khả năng nhúng: Là yêu cầu thứ ba của một hệ giấu tin. Khả năng nhúng chính là số lượng thông tin được nhúng trong phương tiện chứa.

## Steganography trong an toàn thông tin hiện nay

Do kỹ thuật giấu thông tin số mới được hình thành trong thời gian gần đây nên xu hướng phát triển chưa ổn định.

Nhiều phương pháp mới, theo nhiều khía cạnh khác nhau đang và chắc chắn sẽ được đề xuất, bởi vậy một định nghĩa chính xác, một sự đánh giá phân loại rõ ràng chưa thể có được. Sơ đồ phân loại dưới đây được Fabien A. P. Petitcolas đề xuất năm 1999.

Sơ đồ phân loại này như một bức tranh khái quát về ứng dụng và kỹ thuật giấu thông tin. Dựa trên việc thống kê sắp xếp khoảng 100 công trình đã công bố trên một số tạp chí, cùng với thông tin về tên và tóm tắt nội dung của khoảng 200 công trình đã công bố trên Internet, có thể chia lĩnh vực giấu tin ra làm hai hướng lớn, đó là watermarking và steganography.



Hình 1.2. Sơ đồ các hình thức giấu tin

Nếu như watermarking (thủy vân, thủy ấn) quan tâm nhiều đến ứng dụng giấu các mẩu tin ngắn nhưng đòi hỏi độ bền vững lớn của thông tin cần giấu (trước các biến đổi thông thường của tệp dữ liệu môi trường) thì steganography lại quan tâm tới ứng dụng che giấu các bản tin đòi hỏi độ bí mật và dung lượng càng lớn càng tốt. Đối với từng hướng lớn này, quá trình phân loại theo các tiêu chí khác có thể tiếp tục được thực hiện, ví dụ dựa theo ảnh hưởng các tác động từ bên ngoài có thể chia watermark thành hai loại, một loại bền vững với các tác động sao chép trái phép, loại thứ hai lại cần tính chất hoàn toàn đối lập: dễ bị phá huỷ trước các tác động nói trên. Cũng có thể chia watermark theo đặc tính, một loại cần được che giấu để chỉ có một số người tiếp xúc với nó có thể thấy được thông tin, loại thứ hai đối lập, cần được mọi người nhìn thấy.

### Phân loại Steganography trong an toàn thông tin

Trong an toàn thông tin, có rất nhiều phương pháp Steganography mà hầu hết chúng ta đều quen thuộc: Từ mực không màu đến những bức ảnh Microdot,… Với sự phát triển của máy tính và Internet, chúng ta có nhiều cách khác để giấu thông tin hơn trong lĩnh vực an toàn thông tin, chẳng hạn như:

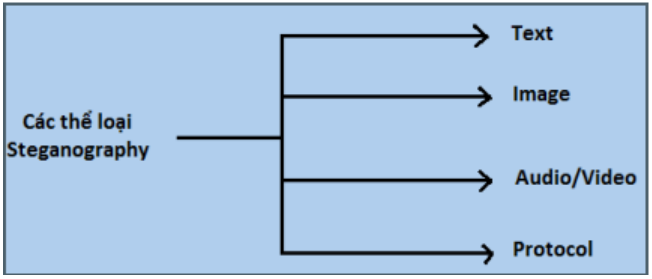
+ Những kênh bí mật. Ví dụ, Loki và một số công cụ từ chối dịch vụ phân tản sử dụng Giao thức ICMP - Internet Control Message Protocol, là kênh truyền thông giữa những kẻ xấu và một hệ thống bị xâm nhập.

+ Ẩn văn bản trong các trang web.

+ Ẩn các tập tin trong các “Plain Sight”. Ví dụ ẩn tập tin với tên là các tập tin âm thanh quan trọng trong thư mục C:\Winnt\System32.

+ Mật khẩu Null. Ví dụ, sử dụng chữ cái đầu tiên của mỗi từ để tạo thành một thông điệp ẩn trong một văn bản vô hại.

Tuy nhiên, Steganography ngày nay phức tạp hơn nhiều so với các ví dụ trên, cho phép người dùng ẩn nhiều lượng thông tin trong các tập hình ảnh và âm thanh. Các hình thức Steganography này thường được sử dụng kết hợp với mật mã để thông tin được bảo vệ kép. Thông tin được mã hóa và ẩn để trước hết kẻ tấn công phải tìm ra thông điệp, một nhiệm vụ thường gặp nhiều khó khăn và sau đó là phải giải mã nó. Hiện nay, có rất nhiều loại phương pháp Steganography và chúng hỗ trợ hầu hết các định dạng tập tin số.



Hình 1.3. Sơ đồ phân loại Steganography

#### Giấu tin trong video

Cũng như giấu thông tin trong ảnh hay trong audio, giấu thông tin trong video đã được quan tâm và phát triển mạnh mẽ cho nhiều ứng dụng như điều khiển truy cập thông tin, xác thực thông tin và bảo vệ bản quyền tác giả, ví dụ như trong các hệ thống chương trình truyền hình có trả phí. Các kỹ thuật giấu tin trong video cũng được phát triển mạnh mẽ và theo hai khuynh hướng là thuỷ vân số và ẩn mã. Một phương pháp giấu tin trong video được đưa ra bởi COX là phương pháp phân bố đều. Ý tưởng cơ bản của phương pháp này là phân phối thông tin giấu dàn trải theo tần số của dữ liệu gốc. Nhiều nhà nghiên cứu đã dùng những hàm số cosin riêng và các hệ số truyền sóng riêng để giấu thông tin. Trong các thuật toán khởi nguồn thì thường chỉ có các kỹ thuật cho phép giấu các ảnh vào trong video, nhưng thời gian gần đây các kỹ thuật mới đã cho phép giấu cả âm thanh và hình ảnh vào trong video.

#### Giấu tin trong audio

Giấu thông tin trong audio mang những đặc điểm riêng, khác với giấu thông tin trong các đối tượng đa phương tiện khác. Một trong những yêu cầu cơ bản của giấu tin là đảm bảo tính chất ẩn của thông tin được giấu đồng thời không làm ảnh hưởng đến chất lượng của dữ liệu gốc. Để đảm bảo yêu cầu này, kỹ thuật giấu thông tin trong ảnh phụ thuộc vào hệ thống thị giác của con người - HVS (Human Vision System) còn kỹ thuật giấu thông tin trong audio lại phụ thuộc vào hệ thống thính giác HAS (Human Auditory System). Và một vấn đề khó khăn ở đây là hệ thống thính giác của con người nghe được các tín hiệu ở các giải tần rộng và công suất lớn nên đã gây khó dễ đối với các phương pháp giấu tin trong audio. Nhưng thật may là HAS lại kém trong việc phát hiện sự khác biệt các dải tần và công suất điều này có nghĩa là các âm thanh to, cao tần có thể che giấu được các âm thanh nhỏ thấp một cách dễ dàng. Các mô hình phân tích tâm lí đã chỉ ra điểm yếu trên và thông tin này sẽ giúp ích cho việc chọn các audio thích hợp cho việc giấu tin. Vấn đề khó khăn thứ hai đối với giấu thông tin trong audio là kênh truyền tin. Kênh truyền hay băng thông chậm sẽ ảnh hưởng đến chất lượng thông tin sau khi giấu. Ví dụ để nhúng một đoạn java applet vào một đoạn audio (16 bit, 44.100 Hz) có chiều dài bình thường thì các phương pháp nói chung cũng cần ít nhất là 20 bit/s. Giấu thông tin trong audio đòi hỏi yêu cầu rất cao về tính đồng bộ và tính an toàn của thông tin. Các phương pháp giấu thông tin trong audio đều lợi dụng điểm yếu trong hệ thống thính giác của con người.

#### Giấu tin trong ảnh

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

• Ảnh phủ: Là ảnh gốc được dùng để nhúng thông tin.

• Thông tin nhúng: Là các thông tin mật cần gửi.

• Ảnh đã nhúng: Là ảnh gốc sau khi đã được nhúng thông tin mật.

• Khóa mật: Là khóa tham gia vào quá trình nhúng, được trao đổi giữa người gửi và người nhận

#### Giấu tin trong văn bản

Giấu thông tin vào các văn bản dạng text khó thực hiện hơn do có ít các thông tin dư thừa, để làm được điều này người ta phải khéo léo khai thác các dư thừa tự nhiên của ngôn ngữ. Một cách khác là tận dụng các định dạng văn bản (mã hóa thông tin và khoảng cách giữa các từ hay các dòng văn bản). Từ nội dung của thông điệp cần truyền đi, người ta cũng có thể sử dụng văn phạm phi ngữ cảnh để tạo nên các văn bản “phương tiện chứa” rồi truyền đi.

### Giới thiệu một số kỹ thuật giấu tin

#### Kỹ thuật giấu tin LSB

LSB (Least Signification Bit) hay còn gọi là bít ít quan trọng nhất, là một kỹ thuật giấu tin được sử dụng phổ biến trong các tập tin hình ảnh. Ý tưởng của thuật toán này là tiến hành giấu tin vào các vị trí bít ít quan trọng nhất của mỗi phần tử trọng bản màu. Đây là phương pháp giấu tin đơn giản nhất, thông điệp dưới dạng nhị phân sẽ được giấu (nhúng) vào các bit LSB - là bit có ảnh hưởng ít nhất tới việc quyết định tới màu sắc của mỗi điểm ảnh. Vì vậy khi ta 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 cũ. Ví dụ đối với ảnh 16bit thì 15bit là biểu diễn 3 màu RGB của điểm ảnh còn bit cuối cùng không dùng đến thì ta sẽ tách bit này ra ở mỗi điểm ảnh để giấu tin…

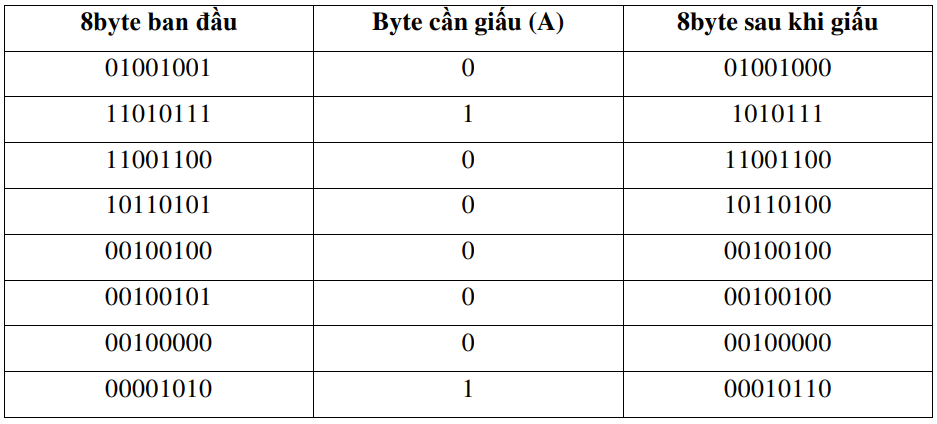
Ví dụ: Tách bit cuối cùng trong 8bit biểu diễn mỗi điểm ảnh của ảnh 256 màu.

Bảng 1.1 Biểu diễn bit ít quan trọng nhất trong kỹ thuật LSB



Trong phép tách này ta coi bit cuối cùng là bit ít quan trọng nhất, thay đổi giá trị của bit này thì sẽ thay đổi giá trị của điểm ảnh lên hoặc xuống đúng một đơn vị, với sự thay đổi nhỏ đó ta hi vọng là cấp độ màu của điểm ảnh sẽ không bị thay đổi nhiều.

Ví dụ thực hiện giấu chữ cái “A” có mã ASCII là 65, được biểu diễn dưới dạng bit là 01000001 vào trong 8 bit của tập tin gốc:

Bảng 1.2 Giấu chữ A vào trong 8 bit đầu của tập tin gốc

**Thuật toán giấu tin đối với Audio:**

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

Đầu ra: Audio đã giấu tin.

Các bước thực hiện:

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

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

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

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

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

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

**Thuật toán tách tin:**

Đầu vào: Audio đã giấu tin S.

Đầu ra: Thông điệp đã giấu M.

Các bước thực hiện:

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

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

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

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

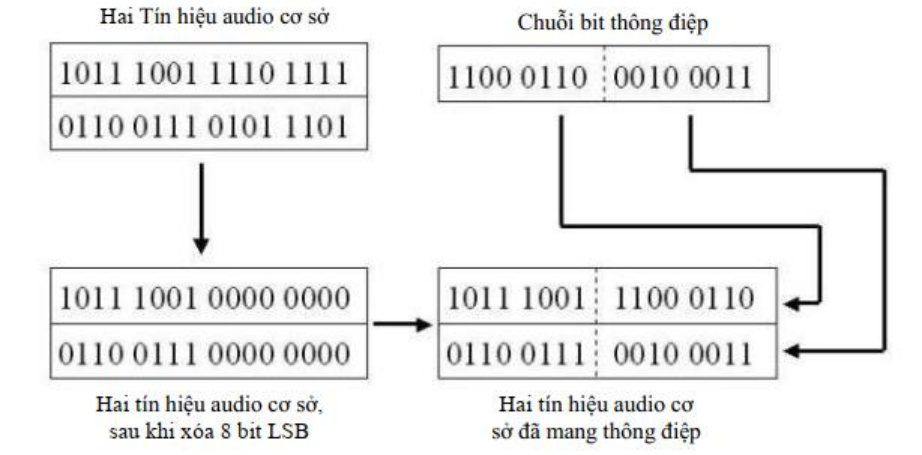
bit, ta được chuỗi bit đã giấu.

**Bước 5**: Chuyển đổi chuỗi bit đã tách về dạng ban đầu ta được thông điệp cần tách.

Thông điệp ban đầu cần giấu có thể là văn bản, dữ liệu ảnh hoặc là một đoạn audio

nào đó. Trong hình 2.3 là một minh họa cho trường hợp số bit LSB của tin hiệu

audio dùng để giấu tin ứng với k=8.



Hình 1.4 Sơ đồ giấu tin trên 8 bit LSB của tín hiệu audio cơ sở

#### Kỹ thuật giấu tin trên miền biến đổi tần số DCT

Kỹ thuật thủy vân sử dụng phép biến đổi DCT thường chia ảnh gốc thành các khối, thực hiện phép biến đổi DCT với từng khối ảnh gốc để được miền tần số thấp, miền tần số giữa và miền tần số cao. Đa số kỹ thuật thủy vân ẩn bền vững sẽ chọn miền tần số giữa của mỗi khối để nhúng bit thủy vân theo một hệ số k nào đó gọi là hệ số tương quan giữa chất lượng ảnh sau khi nhúng thủy vân (tính ẩn của thủy vân) và độ bền vững của thủy vân.

#### Phương pháp Pixel Value Difference (PVD)

Phương pháp Pixel Value Difference (PVD) là một kỹ thuật được sử dụng trong kỹ thuật giấu tin để nhúng thông tin bí mật vào hình ảnh kỹ thuật số. Phương pháp này liên quan đến việc sửa đổi các bit có ý nghĩa nhỏ nhất (LSB) của các giá trị pixel để mã hóa thông tin bí mật.

Phương pháp PVD hoạt động bằng cách so sánh sự khác biệt giữa các giá trị điểm ảnh của các điểm ảnh liền kề nhau trong ảnh. Nếu sự khác biệt giữa hai điểm ảnh liền kề nhỏ hơn một giá trị ngưỡng nhất định, thì LSB của một trong các điểm ảnh được sửa đổi để mã hóa một bit của thông báo bí mật. Quá trình này được lặp lại cho tất cả các cặp điểm ảnh liền kề trong ảnh, cho phép nhúng thông báo bí mật trên toàn bộ ảnh.

Phương pháp PVD là một dạng của kỹ thuật giấu tin miền không gian, vì nó hoạt động trực tiếp trên các giá trị pixel của hình ảnh. Phương pháp này tương đối đơn giản và dễ thực hiện, đồng thời có thể được sử dụng để nhúng một lượng đáng kể thông tin bí mật vào một hình ảnh mà không gây biến dạng có thể nhìn thấy bằng mắt thường.

Tuy nhiên, phương pháp PVD không an toàn lắm vì nó dễ bị tấn công bởi các cuộc tấn công khác nhau như phân tích thống kê, phân tích biểu đồ và phân tích hình ảnh khác biệt. Để cải thiện tính bảo mật của phương pháp PVD, nhiều sửa đổi và cải tiến khác nhau đã được đề xuất, chẳng hạn như Adaptive Pixel Value Difference (APVD), Histogram shifting và permutation-based PVD.

#### Phương pháp Quantized Range Table (QRT)

Phương pháp Quantized Range Table (QRT) là một kỹ thuật được sử dụng trong nén hình ảnh và video để giảm kích thước của hình ảnh và video kỹ thuật số. Phương pháp này liên quan đến việc chia phạm vi giá trị pixel có thể thành một tập hợp các mức lượng tử hóa và sau đó gán từng pixel cho mức tương ứng của nó. Quá trình này được lặp lại cho từng kênh màu trong hình ảnh hoặc video.

Phương pháp QRT sử dụng bảng tra cứu để ánh xạ từng giá trị pixel tới mức lượng tử hóa tương ứng của nó. Bảng này có thể được tạo bằng nhiều thuật toán khác nhau, chẳng hạn như Uniform Quantization, Optimum Mean Square Error (MSE) Quantization và Lloyd-Max Quantization.

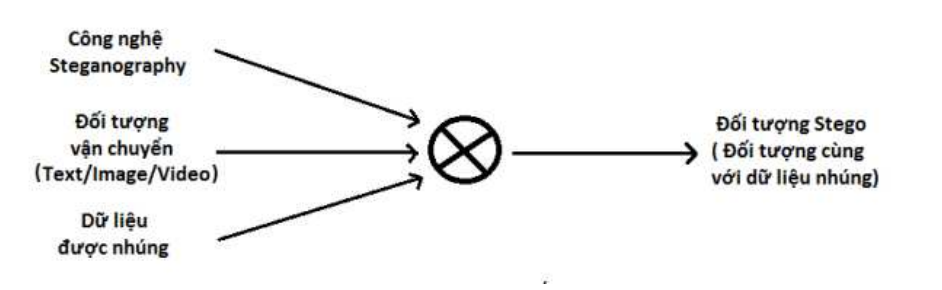
Khi bảng lượng tử hóa đã được tạo, hình ảnh hoặc video được nén bằng cách thay thế từng giá trị pixel bằng mức lượng tử hóa tương ứng. Hình ảnh hoặc video thu được có ít bit trên mỗi pixel hơn, giúp giảm kích thước của nó. Tuy nhiên, việc giảm kích thước này sẽ giảm chất lượng hình ảnh, vì hình ảnh hoặc video được nén có thể có các thành phần nén có thể nhìn thấy được, chẳng hạn như các vùng bị mờ hoặc khối.

Phương pháp QRT được sử dụng trong nhiều tiêu chuẩn nén hình ảnh và video phổ biến, bao gồm JPEG, MPEG và H.264.

### Tầm quan trọng của Steganography trong an toàn thông tin

Steganography có vai trò rất quan trong trong lĩnh vực an toàn thông tin. Nó được sử dụng trong việc che dấu và bảo mật các thông điệp bí mật, quan trọng được truyền gửi trên các môi trường truyền thông như môi trường mạng.

Trong an toàn thông tin, Steganography có liên quan mật thiết với Cryptography. Cryptography là quá trình mã hóa các thông điệp để người khác không thể dễ dàng hiểu được bởi một người không được ủy quyền. Mặt khác, Steganography sẽ ẩn thông điệp để người khác không thể biết về sự tồn tại của thông điệp đó. Nếu một người nào đó xem các đối tượng chứa thông tin ẩn sẽ không thể nghĩ rằng có thông tin được ẩn trong đó. Do đó, họ sẽ không cố gắng để giải mã thông điệp. Quá trình giấu tin trong Steganography được biểu diễn như hình dưới đây.



Hình 1.5 Mô hình chung của quá trình giấu tin Stenography (ẩn mã)

- Các thông điệp bí mật có thể được nhúng vào các đối tượng vận chuyển bởi bộ mã hóa Stegosystem cùng việc sử dụng khóa mật khẩu.

- Một thông điệp bí mật có thể là văn bản thô, văn bản mật mã, một bức ảnh hoặc bất cứ thứ gì khác có thể biểu diễn được dưới dạng một luồng bit.

- Một khi đối tượng vận chuyển được nhúng thông tin vào thì nó được gọi là đối tượng Stego.

- Sau quá trình nhúng, đối tượng Stego được gửi đến người nhận. Người nhận sử dụng bộ giải mã thích hợp cùng với khóa mật khẩu để tìm ra bản gốc của thông điệp người gửi muốn truyền đạt.

Các kỹ thuật Steganography cần bảo đảm các yêu cầu bảo vệ sau:

- Bảo vệ chống lại sự phát hiện (Protection Against Detection) rất cần thiết nếu muốn đảm bảo rằng thông điệp được nhúng không được phát hiện bởi bên thứ ba trái phép.

- Bảo vệ chống lại sự loại bỏ (Protection Against Removal), có nghĩa là cố gắng để ngăn chặn việc loại bỏ các dữ liệu ẩn, không làm hỏng hoặc làm suy giảm chất lượng của nó.

Mặc dù có rất nhiều lợi ích và những công nghệ hiện đại trong Steganography, nhưng trong lĩnh vực truyền thông, việc đảm bảo an toàn thông tin là nhiệm vụ quan trọng nhất. Với sự tiến bộ của công nghệ và việc sử dụng rộng rãi của World Wide Web cho truyền thông đã làm tăng thêm các thách thức trong an ninh, an toàn về thông tin. Các công nghệ tiên tiến đã làm cho các trao đổi thông tin qua mạng an toàn hơn. Nhưng khi mà các công nghệ này không đảm bảo sự tin cậy cho việc truyền thông bí mật trên một khoảng cách dài thì chúng ta cần phải tạo ra một cơ chế an ninh bổ sung. Không thể không kể đến vai trò của hai lĩnh vực Cryptography và Steganography. Chúng giúp bảo mật thông tin ngay cả khi chúng ta bị lộ lọt trong đường truyền. Trong khi Cryptography giữ bí mật thông tin bằng cách thay đổi ý nghĩa và thông tin xuất hiện của thông điệp, thì Steganography sử dụng cơ chế bảo mật bằng cách dấu các thông điệp bí mật vào các thông điệp thông thường khác. Các nội dụng được nhúng làm thay đổi kích cỡ không đáng kể cho các thông điệp bị nhúng. Chính vì các lý do trên, Steganography ngày càng thể hiện sự quan trongcủa mình trong lĩnh vực an toàn thông tin.

Ưu điểm của Steganography là những thông điệp bí mật được chủ ý không để thu hút sự chú ý đến bản thân nó. Rõ ràng ta có thể nhìn thấy các thông điệp đã được mã hóa, tránh được sự tò mò, quan tâm của những người khác.

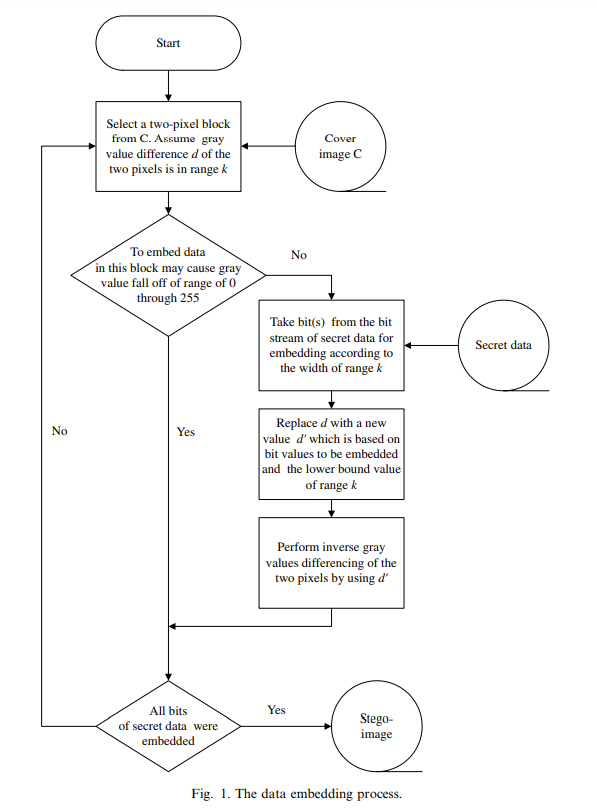
Trong khi Cryptography (mật mã học) chỉ là việc bảo vệ các nội dung của một thông điệp đơn thuần, Steganography còn liên quan với việc che giấu sự thật trong quá trình truyền gửi một thông điệp bí mật, cũng như che giấu nội dung của thông điệp

Steganography làm rất tốt trong việc giấu đi 1 lượng nhỏ dữ liệu bí mật. Hạn chế lớn nhất của Steganography là các tập tin vận chuyển phải lớn hơn đáng kể so với những dữ liệu đã được ẩn. Ví dụ, ta không thể ẩn nội dung của 1 cuốn sách lớn trong 1 tệp hình ảnh nhỏ. Tóm lại, Steganography là kỹ thuật giấu một truyền thông bên trong một truyền thông khác, với mục đích là che giấu những thông điệp bí mật mà không làm ảnh hưởng đến thông điệp chung. Kỹ thuật này giúp người dùng bình thường khó có thể phát hiện và giải mã các thông điệp bí mật được ẩn chứa trong các thông điệp khác, giúp tăng cường tính an toàn thông tin trong quá trình truyền tải dữ liệu.

# ẨN MÃ TRONG ẢNH SỬ DỤNG PHƯƠNG PHÁP PVD VÀ QRT

## Phương pháp PVD

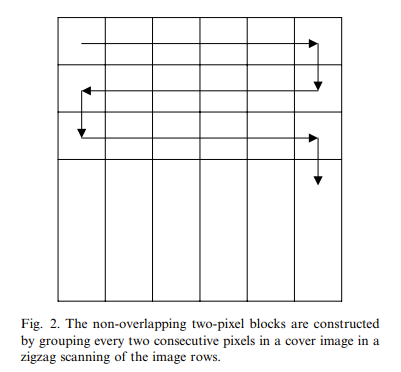
Ẩn dữ liệu trong LSB của các điểm ảnh (pixel) của hình ảnh có giá trị xám (gray-valued image) là một phương pháp ẩn thông tin phổ biến sử dụng đặc tính của khả năng quan sát của con người không nhạy cảm với những thay đổi nhỏ trong hình ảnh. Phương pháp nhúng LSB đơn giản này là dễ dàng tính toán, và một lượng lớn dữ liệu có thể được nhúng mà không ảnh hưởng quá nhiều đến chất lượng. Càng nhiều LSB được sử dụng để nhúng, càng nhiều kết quả bị bóp méo sẽ được tạo ra. Không phải tất cả các điểm ảnh trong một hình ảnh có thể chịu được số lượng thay đổi bằng nhau mà không gây ra sự chú ý cho người quan sát. Số lượng LSB lớn nhất có giá trị xám có thể thay đổi mà không tạo ra một hiện vật có thể cảm nhận được trong mỗi điểm ảnh là khác nhau. Sự thay đổi của các giá trị màu xám của điểm ảnh trong vùng mịn của hình ảnh dễ dàng được mắt người chú ý hơn. Trong phương pháp nhúng Wu Tsai đề xuất, chỉ cần chia ảnh phủ thành một số khối hai điểm ảnh không chồng lên nhau. Mỗi khối được phân loại theo sự khác biệt của các giá trị màu xám của hai điểm ảnh trong khối. Một giá trị khác biệt nhỏ chỉ ra rằng khối nằm trong một vùng mịn và một khối lớn cho biết rằng nó nằm trong một khu vực cạnh. Các điểm ảnh tại khu vực cạnh chịu đựng lớn hơn những thay đổi của giá trị điểm ảnh so với những thay đổi trong khu vực mịn. Vì vậy, trong phương pháp đề xuất, Wu Tsai nhúng thêm dữ liệu trong các khu vực cạnh hơn là trong các khu vực mịn. Và theo cách này, các thay đổi trong hình ảnh stego không gây sự chú ý. Lưu đồ của phương pháp nhúng được đề xuất được phác họa trong Hình 2.1.



Hình 2.1. Quá trình nhúng dữ liệu

### Lượng tử hóa sự khác biệt các giá trị màu xám của khối hai điểm ảnh

Ảnh phủ sử dụng trong phương pháp đề xuất là loại có 256 giá trị màu xám. Một giá trị khác biệt *d* được tính toán từ mọi khối không chồng chéo của hai điểm ảnh liên tiếp, chẳng hạn như *p*i và *p*i+1, của một ảnh phủ. Cách phân vùng ảnh phủ thành các khối hai điểm ảnh chạy qua tất cả các hàng của mỗi hình theo kiểu zigzag, như hình minh họa trong Hình 2.2.



Hình 2.2. Quá trình lấy các khối 2 điểm ảnh không chồng chéo

Giả sử rằng các giá trị xám của *pi* và *pi*+1 lần lượt là *gi* và *gi+1* thì *d* được tính là *gi+1* - g*i*, có thể nằm trong khoảng từ -255 đến 255. Một khối có *d* gần bằng 0 được coi là một khối cực kỳ mịn, trong khi một khối với *d* gần với -255 hoặc 255 được coi là khối cạnh sắc nét. Bằng phương pháp đối xứng, ta chỉ xét các giá trị tuyệt đối có thể có của *d* (0 đến 255) và phân loại chúng thành một số khoảng liền kề, cho *Ri* với *i* = 1, 2, ... , n. Dải giá trị này được gán chỉ số từ 1 đến n. Phía dưới và phía trên các giá trị giới hạn của *Ri* được ký hiệu bởi *li* và *ui* tương ứng, trong đó *li* là 0 và *ui* là 255.

Chiều rộng của *Ri* là *ui* - *li* + 1. Trong phương pháp đề xuất của Wu Tsai, chiều rộng của mỗi khoảng được coi là lũy thừa của 2. Hạn chế về chiều rộng này tạo điều kiện cho việc nhúng dữ liệu nhị phân. Độ rộng của các khoảng đại diện cho các giá trị khác biệt của các khối mịn được chọn **nhỏ hơn** trong khi những giá trị đại diện cho giá trị khác biệt của các khối cạnh được chọn là **lớn hơn**. Vì vậy, Wu Tsai tạo các khoảng với chiều rộng nhỏ hơn khi *d* gần bằng 0 và các khoảng với chiều rộng lớn hơn khi *d* cách xa 0 cho mục đích mang lại kết quả tốt hơn.

Một giá trị chênh lệch nằm trong khoảng có chỉ số *k* là được cho là có chỉ số *k*. Tất cả các giá trị trong một số khoảng (nghĩa là tất cả các giá trị có chỉ mục giống hệt nhau) được coi là *đủ gần*. Nghĩa là, nếu một giá trị chênh lệch trong một khoảng được thay thế bằng một giá trị khác trong cùng một khoảng, sự thay đổi gần như không thể nhận thấy bởi mắt người. Trong phương pháp đề xuất, Wu Tsai nhúng một số bit của thông điệp bí mật vào trong một khối hai điểm ảnh bằng cách thay thế sự khác biệt giá trị của khối với một khối có chỉ mục giống hệt nhau, tức là, thay đổi một giá trị khác biệt trong một khoảng thành bất kỳ giá trị chênh lệch nào trong cùng một khoảng đó. Nói cách khác, trong quá trình nhúng dữ liệu được đề xuất, Wu Tsai điều chỉnh các giá trị màu xám trong mỗi cặp hai điểm ảnh bằng hai giá trị mới có giá trị chênh lệch gây ra những thay đổi không thể nhận thấy đối với một người quan sát hình ảnh stego.

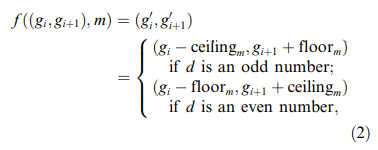
### Quá trình nhúng dữ liệu

Coi thông điệp bí mật là một chuỗi các bit. Muốn nhúng từng bit trong chuỗi bit bí mật vào các khối hai điểm ảnh của ảnh phủ. Số bit có thể được nhúng trong mỗi khối là khác nhau và được quyết định bởi chiều rộng của phạm vi mà giá trị chênh lệch của hai điểm ảnh trong khối thuộc về. Cho một khối hai điểm ảnh B với chỉ số *k* và chênh lệch giá trị xám *d*, số lượng bit là *n* có thể nhúng trong khối này được tính bằng *n* = log2 (*u*k – *l*k + 1). Vì chiều rộng của mỗi phạm vi được chọn là một lũy thừa của 2, giá trị *n* = log2 (*u*k – *l*k + 1) là một số nguyên. Một chuỗi con *S* có *n* bit tiếp theo được chọn từ thông điệp bí mật để nhúng vào B. Một giá trị khác biệt *d’* sau đó được tính bằng công thức:



Trong đó *b* là giá trị của chuỗi con S. Bởi vì giá trị *b* nằm trong khoảng từ 0 đến *u*k – *l*k , giá trị của *d’* nằm trong phạm vi từ *lk* đến *uk* . Nếu chúng ta thay thế *d* bằng *d’*, những thay đổi dẫn đến không đáng chú ý đối với người quan sát. Sau đó nhúng *b* bằng cách thực hiện một phép tính nghịch đảo từ *d’* được mô tả bên cạnh số các giá trị màu xám mới (*g’i* , *g’i+1*) cho các điểm ảnh trong khối hai điểm ảnh tương ứng (*p’i* , *p’i+1*) của hình ảnh stego. Quá trình nhúng kết thúc khi tất cả các bit của thông điệp bí mật được nhúng.

Phép tính nghịch đảo để tính toán (*g’i* , *g’i+1*) từ các giá trị màu xám ban đầu (*gi* , *gi+1*) của cặp điểm ảnh dựa trên một hàm *f ((gi , gi+1), m*) được định nghĩa là



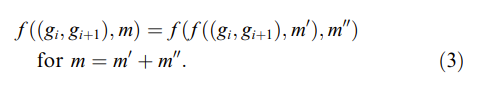
trong đó *m = d’ - d*, ceiling*m* = ⸢ *m/2*⸣ (làm tròn cận trên), và floor*m* = ⸤ *m/2*⸥ (làm tròn cận dưới). Phương trình trên thỏa mãn yêu cầu là hiệu giữa *g’i* và *g’i+1* là *d’*. Lưu ý rằng một chính sách giảm biến dạng đã được sử dụng trong việc thiết kế phương trình (2) để tạo ra *g’i* và *g’i+1*  từ *gi* và *gi+1* để biến dạng gây ra bằng cách thay đổi *gi* và *gi+1* được phân bổ gần như bằng nhau trên hai điểm ảnh trong khối. Kết quả là giá trị màu xám thay đổi trong khối thì ít bị nhận thấy hơn.

Trong phép tính nghịch đảo ở trên, một giá trị nhỏ hơn của *d’* tạo ra một khoảng nhỏ hơn giữa *g’i* và *g’i+1* trong khi *d’* lớn hơn tạo ra khoảng lớn hơn. Vì vậy, (*gi* và *gi+1*) có thể tạo ra (*g’i* và *g’i+1* ) không hợp lệ. Nghĩa là, một số tính toán có thể gây ra kết quả *g’i* hoặc *g’i+1* nằm ngoài ranh giới của phạm vi [0, 255].

Mặc dù có thể điều chỉnh lại hai giá trị mới thành nằm trong phạm vi hợp lệ là [0, 255] đồng thời điều chỉnh giá trị kia thành giá trị phù hợp để thỏa mãn sự khác biệt *d’*, nhưng điều này có thể tạo ra điểm bất thường tương phản với xung quanh vùng trong một số trường hợp. Để giải quyết vấn đề này, sử dụng quy trình kiểm tra để phát hiện các trường hợp nằm ngoài ranh giới như vậy và loại bỏ các khối điểm ảnh mang lại những trường hợp như vậy để nhúng dữ liệu. Các giá trị màu xám của các khối bị bỏ được giữ nguyên trong hình ảnh stego. Chiến lược này giúp dễ dàng phân biệt các khối có dữ liệu được nhúng với các khối bị bỏ trong quá trình khôi phục dữ liệu từ một hình ảnh stego, sẽ được thảo luận trong phần tiếp theo. Cần lưu ý rằng điểm ảnh bị bỏ như vậy trong các khối rất ít trong ứng dụng thực tế theo các thí nghiệm.

Kiểm tra vượt ranh giới được đề xuất tiến hành bằng cách tạo ra một cặp (ĝ *i* và ĝ *i+1* ) từ phép tính nghịch đảo giá trị của hàm số *f ((gi , gi+1), uk­ - d*). Vì *uk* là giá trị lớn nhất trong phạm vi từ *lk* đến *uk* , kết quả là cặp (ĝ *i* và ĝ *i+1* ) được tạo ra bằng cách sử dụng *uk* sẽ mang lại chênh lệch tối đa. Phạm vi tối đa trong khoảng từ ĝ *i+1* - ĝ *i* bao gồm tất cả các phạm vi mang lại bởi các cặp (ĝ *i* và ĝ *i+1*) khác. Vì vậy, việc kiểm tra khối nằm ngoài ranh giới có thể tiến hành bằng cách chỉ kiểm tra các giá trị của (ĝ *i* và ĝ *i+1*), được sinh ra bởi trường hợp sử dụng *uk* Nếu ĝ *i+1* hoặc ĝ *i* nằm ngoài ranh giới của 0 hoặc 255, coi khối đó có khả năng nằm ngoài phạm vi cho phép và không nhúng dữ liệu khối đó.

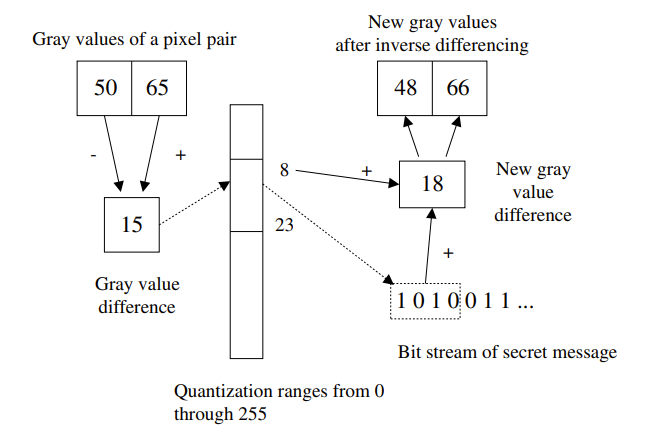
Ngoài ra, phép tính nghịch đảo trong biểu thức (2) được thiết kế sao cho nó thỏa mãn tính chất sau:



Phương trình này có nghĩa là phép tính nghịch đảo có thể tiến hành trực tiếp hoặc lũy tiến. Điều này hữu ích để đánh giá sự tồn tại của dữ liệu được nhúng trong mỗi khối trong quá trình khôi phục dữ liệu.

Minh họa quá trình nhúng dữ liệu được hiển thị trong Hình 2.3. Trong hình, các giá trị màu xám của một khối hai pixel mẫu được ví dụ là (50, 65). Giá trị chênh lệch là 15, nằm trong phạm vi từ 8 đến 23. Chiều rộng của phạm vi là

16 = 24 , có nghĩa là một giá trị chênh lệch trong phạm vi có thể được sử dụng để nhúng 4 bit dữ liệu bí mật. Giả sử rằng bốn bit đầu của dữ liệu bí mật là 1010. Giá trị của luồng bit này là 10 (DEC). Nó được cộng với giá trị giới hạn dưới 8 của phạm vi để mang lại giá trị chênh lệch mới 18. Cuối cùng, bằng phương trình (2) các giá trị (48, 66) được tính để sử dụng như các giá trị màu xám trong hình ảnh stego. Để ý rằng 66 - 48 = 18.



Hình 2.3. Ví dụ minh họa cho quá trình nhúng dữ liệu

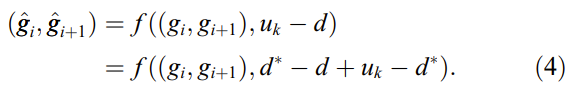
### Quá trình trích xuất thông tin từ ảnh stegano

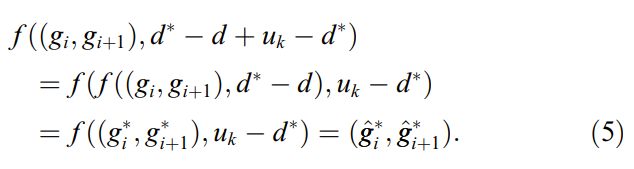
Quá trình trích xuất thông điệp được nhúng tiến hành bằng cách sử dụng seed của lược đồ giả ngẫu nhiên để tạo ra cùng một lượt duyệt để truy cập các khối hai pixel như trong quá trình nhúng. Mỗi lần truy cập một khối hai pixel trong hình ảnh stego, chúng tôi áp dụng kiểm tra ngoài ranh giới tương tự như đã đề cập trước đó cho khối để tìm hiểu xem liệu khối đó đã được sử dụng trong quá trình nhúng hay không. Cho rằng khối trong hình ảnh stego có giá trị màu xám (, ) và giá trị khác biệt d\* của hai giá trị màu xám có chỉ mục *k*. Áp dụng các quá trình kiểm tra vượt quá ranh giới cho (, ) bằng cách sử dụng

*f ((, ), uk – d\*).*

Bây giờ chúng ta muốn chứng minh rằng kết quả ( tính từ *f ((, ), uk – d\*)* là giống với các giá trị màu xám (ĝ *i* và ĝ *i+1* ) được tính bởi *f ((gi , gi+1), uk­ - d*) trong quá trình nhúng.

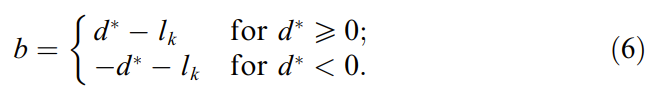
Chứng minh: Đầu tiên,



bằng phương trình (3) đã nêu từ trước, kết quả trên có thể biến đổi hơn nữa đến: 

Điều này hoàn tất chứng minh mệnh đề.

Tính chất trên cho thấy kết quả của cả hai quy trình kiểm tra vượt quá ranh giới, một trong quá trình nhúng dữ liệu và một trong trích xuất dữ liệu là giống hệt nhau. Điều này lần lượt ngụ ý rằng nếu một trong hai giá trị màu xám của giá trị được tính toán ( nằm ngoài ranh giới của phạm vi [0, 255], điều đó có nghĩa là khối hiện tại không được sử dụng để nhúng dữ liệu hoặc khối đó đã bị bỏ trong quá trình nhúng. Ngược lại, nếu cả hai giá trị ( không nằm ngoài phạm vi, điều đó có nghĩa là một số dữ liệu đã được nhúng trong khối. Giá trị *b*, được nhúng trong khối hai pixel này, sau đó được trích xuất sử dụng phương trình:



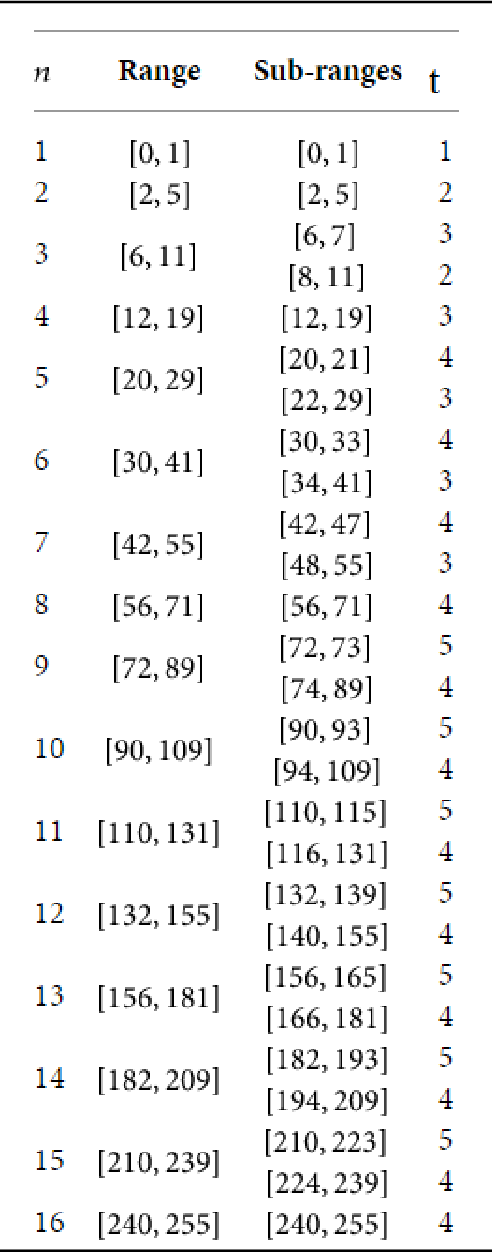
Lưu ý rằng trong quá trình khôi phục thông điệp bí mật từ hình ảnh stego bằng cách sử dụng quy trình trích xuất được mô tả trước đó, không cần tham chiếu đến ảnh phủ.

## Phương pháp QRT

Bảng phạm vi lượng tử hóa (QRT) là một phương pháp được sử dụng trong kỹ thuật ghi ảnh để ẩn thông tin bí mật trong một hình ảnh. Phương pháp QRT được sử dụng để ẩn thông tin trong các bit giá trị pixel ít quan trọng nhất trong một hình ảnh.

Ý tưởng cơ bản đằng sau phương pháp QRT là chia các giá trị pixel trong hình ảnh thành nhiều phạm vi, sau đó ánh xạ từng phạm vi thành một tập hợp bit cụ thể sẽ được sử dụng để ẩn thông tin bí mật. Số lượng bit được sử dụng để ẩn thông tin bí mật phụ thuộc vào kích thước của phạm vi và mức độ bảo mật mong muốn.

Phương pháp QRT có thể được triển khai bằng cách sử dụng bảng lượng tử ánh xạ các giá trị pixel tới các phạm vi cụ thể.



Được thiết kế mới dựa trên số ô vuông hoàn hảo và được mô tả trong bảng trên. Đối với mỗi chênh lệch giá trị pixel, chọn số ô vuông hoàn hảo gần nhất n, sau đó chúng ta có phạm vi n2-n <= n2 < n2+n-1 cho n[1,16]. Độ rộng của phạm vi này là n2 + n - n2 – n = 2n và độ dài bit nhúng là t=[log22n]. Đối với mỗi dải ô, nếu chiều rộng của dải ô lớn hơn 2t, thì chúng ta chia dải ô này thành hai dải con : [n2 – n , n2 + n – 2t] và [n2 + n – 2t +1 , n2 + n - 1].

Theo định nghĩa của dải con, nếu các bit được nhúng t+1 bằng một trong số t+1 bit LSB trong dải con đầu tiên, thì chúng ta có thể nhúng t+1 bit là dải con đầu tiên. Mặt khác, dải phụ thứ hai được sử dụng với khả năng nhúng t.

### Kĩ thuật nhúng

Bước 1: Chọn một tấm ảnh phủ có kích thước 512\*512.

Bước 2: Đọc ảnh phủ này.

Bước 3: Phân vùng ảnh phủ để giấu thông tin thành từng đoạn. Một phân đoạn bao gồm cặp hai pixel không chồng chéo liên tiếp.

Bước 4: Tính giá trị chênh lệch 'di' cho từng đoạn của hai pixel không chồng lấp liên tiếp pi và p(i+1). Giá trị này được cho bởi di=|pi - p(i+1)|.

Bước 5: Tiếp theo, tìm hai giá trị chênh lệch cao nhất không được tạo bởi giá trị Pixel chung.

Bước 6: Tìm số n vuông hoàn hảo gần nhất cho hai giá trị chênh lệch và tính toán độ dài của các bit nhúng t =[log22n]. Có hai trường hợp: Tìm kiếm dải con đầu tiên và tìm giá trị p trong dải con sao cho LSB(p, t+1) = Secret (t+1) rồi đặt d’=p. Mặt khác, tìm kiếm dải con thứ hai và tìm p trong dải con sao cho LSB (p, t) = Secret (t) và sau đó đặt d’=p.

Bước 7: Tính hiệu giữa di' và di để tìm giá trị của m.

Bước 8: Bây giờ sửa đổi các giá trị pixel của từng cặp theo PVD cơ bản được mô tả trước đó.

Bước 9: Lặp lại các bước từ 4 đến 12 để nhúng toàn bộ dữ liệu bí mật vào các phân đoạn.

Ví dụ: chúng ta chọn phân đoạn có các giá trị pixel sau:

|  |  |
| --- | --- |
| 164 | 186 |
| 142 | 172 |

Tính giá trị chênh lệch giá trị giữa các pixel:

d1=22 ; d2=14; d3=30; d4=22

Chọn các giá trị chênh lệch pixel cao nhất không có pixel chung, tức là d1=22 và d3=30. Số bình phương hoàn hảo gần nhất cho cả hai giá trị chênh lệch là n=5 và không. của các bit có thể được nhúng t=log2(2n)=3. Hai điều kiện sau đây được thảo luận.

Trường hợp 1 : Dữ liệu bí mật là “0100” hoặc “0101”

Trong dải phụ đầu tiên cho giá trị n đã chọn [20,21] và không. số bit được nhúng là t+1=4, bốn LSB giống như dữ liệu bí mật. Giả sử dữ liệu được nhúng là “0101”, thì giá trị chênh lệch mới sẽ là d1'=21[00010101].m=d1'-d1=1 và các giá trị pixel đã sửa đổi là [165,186].

Trường hợp 2: Dữ liệu bí mật là “011”

Trong phạm vi phụ đầu tiên không có LSB phù hợp, vì vậy chúng tôi sẽ chuyển sang phạm vi phụ thứ hai [22,29] và không. số bit được nhúng là t=3. Giá trị chênh lệch mới từ dải con là d3’=27[00011011] và m=d3’-d3=3. Các giá trị pixel đã sửa đổi là [144,171].

### Kĩ thuật trích xuất

Các bước sau đây được sử dụng để trích xuất dữ liệu ẩn như sau:

Bước 1: Đọc stego –image.

Bước 2: Phân vùng ảnh stego thành các phân đoạn pixel bao gồm cặp hai pixel không chồng chéo liên tiếp.

Bước 3: Tiếp theo, tính giá trị chênh lệch di của hai pixel liên tiếp của mỗi đoạn bằng cách sử dụng công thức di=|pi-pi+1| .

Bước 4: Tìm hai giá trị chênh lệch cao nhất không được tạo bởi một giá trị pixel chung.

Bước 5: Tìm khoảng Ri thích hợp cho sự khác biệt di.

Bước 6: Tìm số n vuông hoàn hảo gần nhất cho hai giá trị chênh lệch và tính toán độ dài của các bit nhúng t =[log22n]. Tìm kiếm dải phụ và xác định dải phụ đó thuộc về dải nào và trích xuất dữ liệu bí mật (secret(t+1)) = (LSB d',t+1) cho dải phụ đầu tiên và (secret t) = (LSB d', t) cho phạm vi con thứ hai. Cuối cùng, chúng ta trích xuất tất cả dữ liệu bí mật.

Bước 7: Sau đó, những thông tin nhị phân này được chuyển thành chuỗi. Chuỗi này được gọi là thông tin gốc.

Ví dụ: chúng ta đã chọn cùng một phân khúc với các giá trị pixel sau:

|  |  |
| --- | --- |
| 165 | 186 |
| 144 | 171 |

Tính giá trị chênh lệch giá trị giữa các pixel:

d1=21 ; d2=15; d3=27; d4=21

Chọn các giá trị chênh lệch pixel cao nhất không có pixel chung, tức là d1=21 và d3=27. Số bình phương hoàn hảo gần nhất cho cả hai giá trị chênh lệch là n=5. Không có bit nào được nhúng trong cặp pixel là t+1=4 (t=log2(2n)) cho dải con thứ nhất và t=3 cho dải con thứ hai

Đối với giá trị chênh lệch thứ nhất d1=21 từ dải con đầu tiên, do đó, dữ liệu nhúng bí mật là bốn LSB cuối cùng của 21 tức là 0101 và đối với giá trị chênh lệch thứ hai d3=27, dữ liệu nhúng bí mật là ba LSB cuối cùng của 27 tức là 011. Giống như tất cả các bit bí mật này được phục hồi.

### Ưu, nhược điểm

Phương pháp QRT có thể được sử dụng để che giấu nhiều loại thông tin bí mật, bao gồm văn bản, hình ảnh và âm thanh. Tuy nhiên, điều quan trọng cần lưu ý là phương pháp QRT có thể dễ bị tấn công liên quan đến phân tích thống kê hình ảnh, chẳng hạn như phát hiện các giá trị pixel hoặc mẫu bit bất thường.

Để nâng cao tính bảo mật của phương pháp QRT, có thể sử dụng một số kỹ thuật, chẳng hạn như thêm nhiễu vào các giá trị pixel, sử dụng bảng lượng tử hóa khác nhau cho mỗi thông báo hoặc sử dụng kết hợp nhiều kỹ thuật nhúng. Điều quan trọng cần lưu ý là tính bảo mật của bất kỳ kỹ thuật lưu trữ dữ liệu nào đều phụ thuộc vào việc triển khai và bối cảnh mà nó được sử dụng.

Ưu điểm của phương pháp QRT là nó tương đối đơn giản và hiệu quả để thực hiện. Nó có thể được sử dụng để ẩn thông tin bí mật trong nhiều định dạng hình ảnh, bao gồm JPEG, BMP và PNG.

Ưu điểm tiếp theo là nó không làm thay đổi đáng kể diện mạo trực quan của hình ảnh. Điều này có thể quan trọng trong một số ứng dụng mong muốn ẩn thông tin mà không gây chú ý đến thực tế là một hình ảnh đã được sửa đổi.

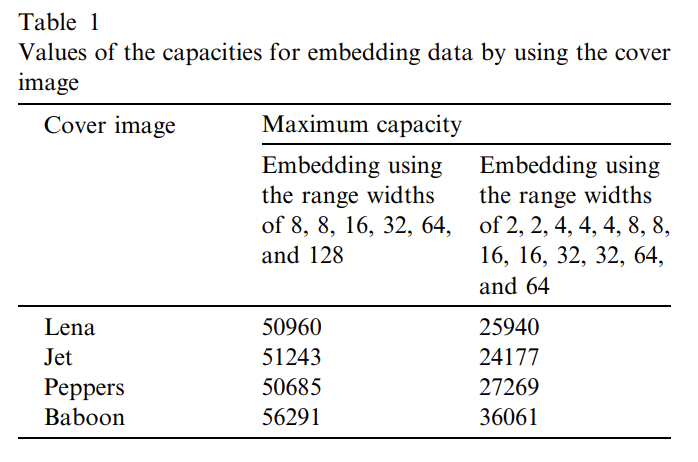
Tuy nhiên, có một hạn chế của phương pháp QRT là nó có thể dễ bị tấn công liên quan đến phân tích thống kê hình ảnh. Ví dụ: kẻ tấn công có thể phát hiện các mẫu hoặc giá trị pixel bất thường cho biết sự hiện diện của thông tin ẩn. Để giảm thiểu lỗ hổng này, có thể sử dụng nhiều kỹ thuật khác nhau, chẳng hạn như thêm nhiễu vào các giá trị pixel, sử dụng bảng lượng tử hóa khác nhau cho mỗi thông báo hoặc sử dụng kết hợp nhiều kỹ thuật nhúng.

Một hạn chế khác của phương pháp QRT là nó chỉ có thể được sử dụng để che giấu một lượng thông tin bí mật tương đối nhỏ trong một hình ảnh. Điều này là do số lượng bit có thể được sử dụng để ẩn thông tin bí mật bị giới hạn bởi kích thước của phạm vi pixel và mức độ bảo mật mong muốn.

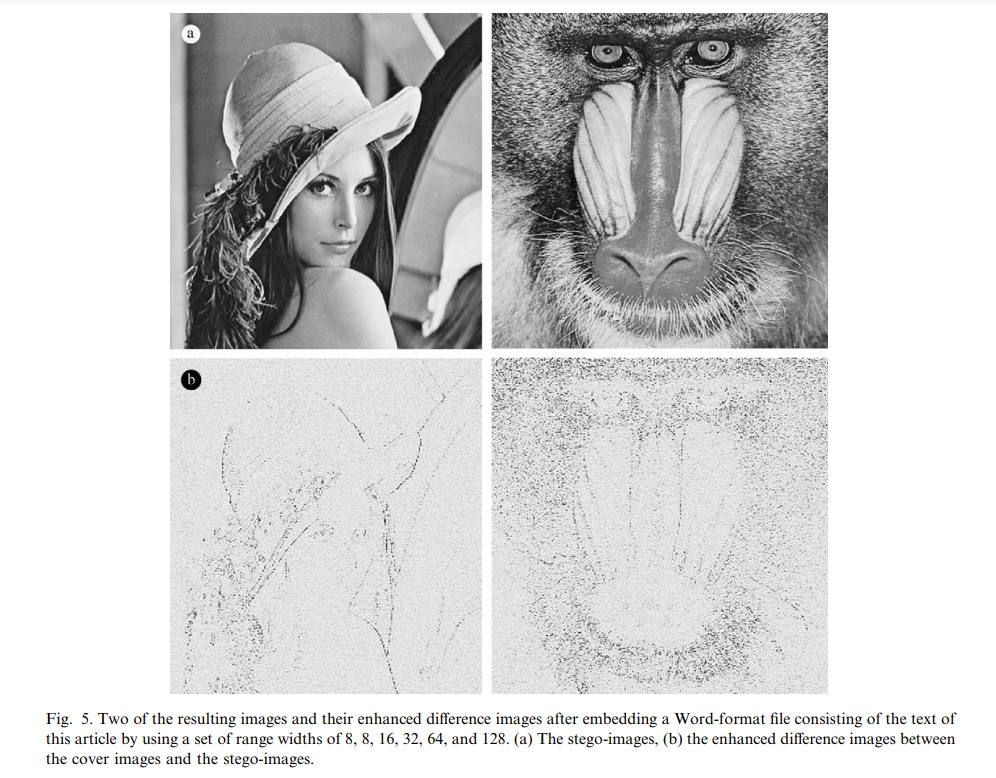
# THỰC NGHIỆM

## Kết quả thực nghiệm phương pháp PVD

Trong các thử nghiệm, bốn ảnh phủ ''Lena'', ''Jet'', ''Peppers'', và ''Baboon'' đã được sử dụng, mỗi ảnh có kích thước 512 x 512. Hai trong số chúng được hiển thị trong Hình 4. Hai tập hợp độ rộng của phạm vi sự khác biệt giá trị màu xám đã được sử dụng trong các thí nghiệm. Đầu tiên thử nghiệm được dựa trên việc lựa chọn phạm vi chiều rộng 8, 8, 16, 32, 64 và 128, phân vùng tổng phạm vi [0, 255] thành [0, 7], [8, 15], [16; 31], ... , [128, 255]. Thí nghiệm thứ hai dựa trên việc sử dụng độ rộng phạm vi 2, 2, 4, 4, 4, 8, 8, 16, 16, 32, 32, 64 và 64. Các giá trị của khả năng nhúng dữ liệu bằng cách sử dụng ảnh phủ và hai bộ độ rộng phạm vi được đưa ra trong Bảng 1.

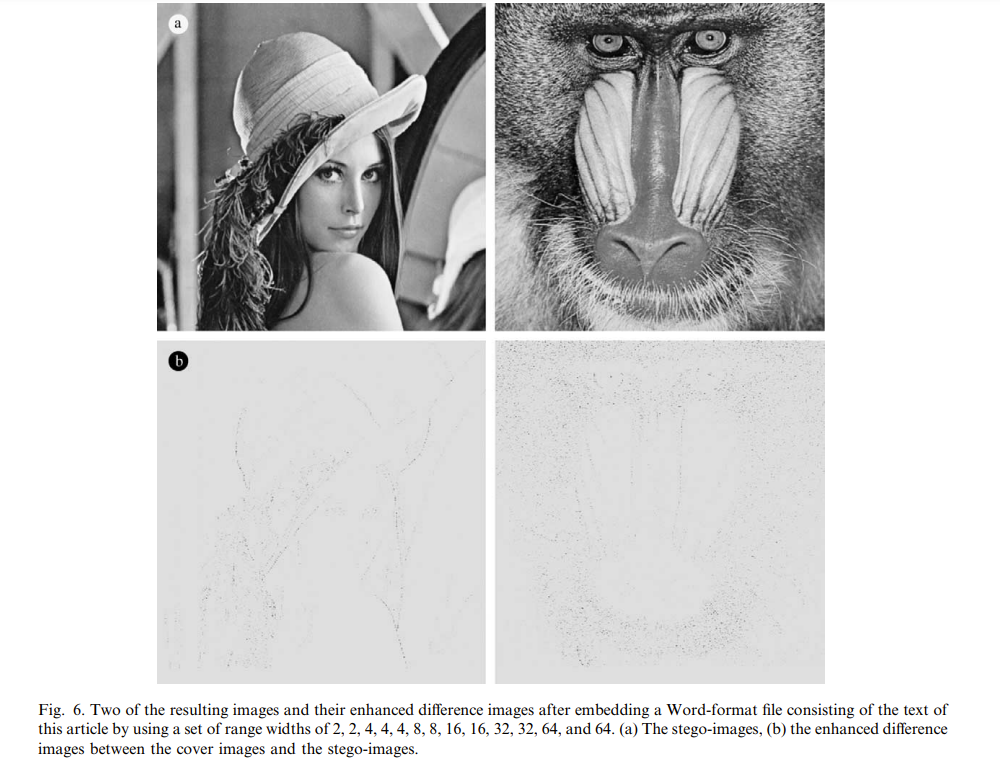


Wu-Tsai đã sử dụng tệp có định dạng Word chứa các văn bản của tài liệu là thông điệp bí mật trong các thí nghiệm. Một số kết quả củat hí nghiệm đầu tiên được hiển thị trong Hình 3.1.



Hình 3.1

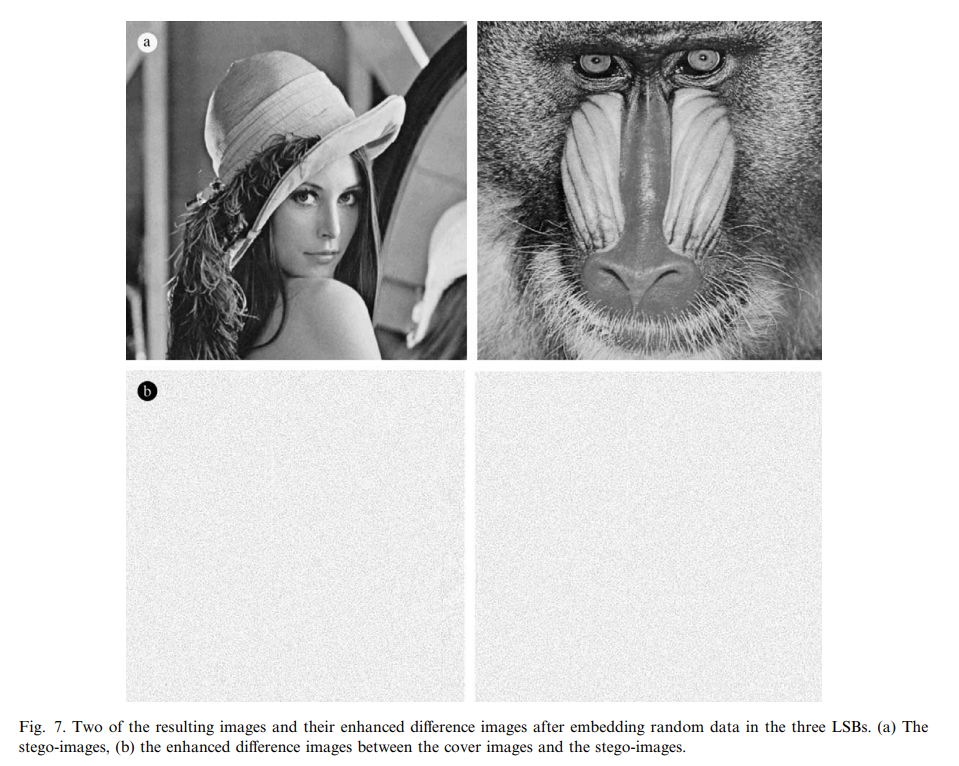
Trong Hình 3.1 (a) hiển thị hai trong số các kết quả hình ảnh stego được nhúng dữ liệu bí mật đã cho bằng cách sử dụng bộ đầu tiên về độ rộng phạm vi và trong Hình 3.1(b), chúng tôi hiển thị hình ảnh khác biệt nâng cao tương ứng giữa các hình ảnh gốc của Hình 3.1(a) và các hình ảnh phủ của hình ban đầu (với sự khác biệt của các giá trị màu xám là được chia tỷ lệ năm lần). Tương tự kết quả của thí nghiệm lần thứ hai được thể hiện trong Hình 3.2.



Hình 3.2

Sự khác biệt hình ảnh được hiển thị ở đây để chỉ ra các biến dạng kết quả từ quá trình nhúng dữ liệu. Từ chúng, chúng ta thấy rằng hầu hết các biến dạng được tìm thấy trên các cạnh trong hình ảnh. Điều này có nghĩa là biến dạng sẽ ít được chú ý hơn vì những thay đổi ở các phần cạnh của hình ảnh thường ít rõ ràng hơn đối với mắt người.

Ngược lại, với mục đích so sánh, hai hình ảnh stego do nhúng ngẫu nhiên dữ liệu vào ba LSB của các giá trị pixel bằng cách sử dụng kỹ thuật nhúng LSB truyền thống và các hình ảnh khác biệt nâng cao tương ứng được hiển thị trong Hình 3.3.

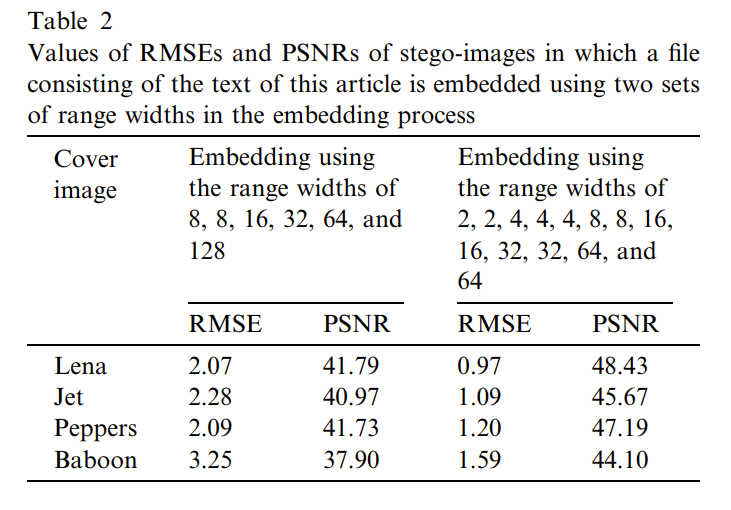


Hình 3.3

Có thể thấy được rằng các biến dạng được *lan truyền khắp hình ảnh,* điều này rõ ràng hơn đối với người quan sát so với biến dạng do phương pháp PVD bị hạn chế về cơ bản ở các khu vực cạnh, như trong Hình 3.1 và 3.2.

Tất cả các kết quả được tạo ra bằng cách nhúng dữ liệu bí mật trong các khối hai pixel của ảnh phủ theo thứ tự duyệt ngang ngẫu nhiên được tạo bởi một sơ đồ giả ngẫu nhiên, đi qua ảnh phủ và chỉ truy cập từng khối hai pixel một lần.

Cuối cùng, các giá trị của các đỉnh của nhiễu tín hiệu (PSNR) và lỗi bình phương trung bình gốc (RMSE) của kết quả nhúng được hiển thị trong Bảng 2.



Chất lượng vẫn tốt ngay cả trong ảnh gốc với PSNR thấp hơn.

# KẾT LUẬN

Ba chương của đề tài này đã thể hiện được rằng những mục tiêu đặt ra khi thực hiện đề tài đều đã đạt được. Cụ thể:

Chương 1 Đã giới thiệu về kỹ thuật giấu tin, các khái niệm cơ bản trong kỹ thuật giấu tin và trong an toàn thông tin hiện nay

Chương 2 Trình bày về ẩn mã trong ảnh với hai phương pháp PVD và QRT

Chương 3 Đã trình bày kết quả thực nghiệm sử dụng phương pháp PVD

Ngoài ra, qua quá trình nghiên cứu và thực hiện đề tài cũng đã mang lại rất nhiều kiến thức và kỹ năng làm việc nhóm cho chúng em. Đây là một trong những cơ hội quý giá giúp sinh viên phát triển và hoàn thiện bản thân. Dù vậy, quá trình thực nghiệm vẫn còn nhiều vấn đề liên quan mà nghiên cứu này chưa thực hiện được. Việc tiếp tục phát triển và hoàn thiện hơn những vấn đề còn tồn tại cũng chính là hướng phát triển tương lai của đề tài.

# TÀI LIỆU THAM KHẢO

**[1]** A steganographic method for images by pixel-value differencing [Da-Chun Wu, Wen-Hsiang Tsai]

**[2]** H.W.Tseng and H.S.Leng,”A Steganographic Method Based on Pixel Value Differencing and Perfect SquareNumber” Hindwai Journal of Applied Mathematics, 2013

**[3]** J. K. Mandal and Debashis Das, “Steganography Using Adaptive Pixel Value Differencing (APVD) of Gray Images Through Exclusion of Overflow/Underflow.” CCSEA, EA, CLOUD, DKMP, CS & IT 05, pp. 93– 102, 2012.

**[4]** Lee YP, Lee J-C, ChenW-K, Chang K-C, Su I-J, Chang C-P, "High Payload Image Hiding With Quality Recovery Using Tri-Way Pixel Value Differencing," Information Sciences, vol. 191, pp. 214-225, 2012.