# Bìa 1

# Bìa 2

# LỜI CẢM ƠN

# LỜI CAM ĐOAN

# LỜI MỞ ĐẦU

# MỤC LỤC

[Bìa 1 1](#_Toc59520525)

[Bìa 2 2](#_Toc59520526)

[lời cảm ơn 3](#_Toc59520527)

[lời cam đoan 4](#_Toc59520528)

[lời mở đầu 5](#_Toc59520529)

[MỤC LỤC 6](#_Toc59520530)

[bảng viết tắt 9](#_Toc59520531)

[mục lục hình ảnh 11](#_Toc59520532)

[Chương I : Giới Thiệu 12](#_Toc59520533)

[1.1. Giới Thiệu Nội Dung Đề Tài 12](#_Toc59520534)

[1.2. Mục Tiêu Nội Dung Đề Tài 13](#_Toc59520535)

[1.3. Giới Hạn Đề Tài 13](#_Toc59520536)

[1.4. Cấu Trúc Báo Cáo 14](#_Toc59520537)

[Chương II : Cơ Sở Lý Thuyết và Các Nghiên Cứu Liên Quan 16](#_Toc59520538)

[2.1 Cơ Sở Lý Thuyết 16](#_Toc59520539)

[2.1.1 Định Nghĩa 16](#_Toc59520540)

[2.1.2 Vài nét về lịch sử giấu tin. 16](#_Toc59520541)

[2.1.3 Mô hình kỹ thuật giấu tin và các thuật ngữ cơ bản 17](#_Toc59520542)

[2.1.4 Sự khác biệt giữa mã hóa và giấu tin. 19](#_Toc59520543)

[2.1.5 Giấu tin trong dữ liệu đa phương tiện 20](#_Toc59520544)

[2.2. Các Nghiên Cứu Liên Quan 30](#_Toc59520545)

[2.2.1. Kỹ thuật thuỷ vân sử dụng phép biến đổi cosin rời rạc 30](#_Toc59520546)

[2.1.2 Kỹ thuật thủy vân của Shoemarker C. 32](#_Toc59520547)

[2.2.2 Một số kỹ thuật thủy vân sử dụng phép biến đổi sóng nhỏ 35](#_Toc59520548)

[2.2.3 Kỹ thuật thuỷ vân của Mehul R. và Priti R. 36](#_Toc59520549)

[2.2.4. Kỹ thuật thuỷ vân của Tao P. và Eskicioglu A. M. 39](#_Toc59520550)

[2.2.5. Thuật toán SW (Simple Watermarking). 41](#_Toc59520551)

[2.2.6. Thuật toán WU-LEE 45](#_Toc59520552)

[Chương III : Phương Pháp Nghiên Cứu Cơ Chế Giấu Tin Trong Ảnh và Ứng Dụng Trong Mã hóa Dữ Liệu 50](#_Toc59520553)

[3.1. Yêu Cầu bài Toán 50](#_Toc59520554)

[3.2. Phương Pháp Đề Xuất 50](#_Toc59520555)

[3.2.1. Giới thiệu về kỹ thuật thủy vân LBS(Least Signification Bit) 50](#_Toc59520556)

[3.2.2. Quá trình nhúng thủy vân. 52](#_Toc59520557)

[3.2.3. Quá trình tách thủy vân. 53](#_Toc59520558)

[3.3. Phương Pháp Đánh Giá 56](#_Toc59520559)

[3.3.1. Test vector 56](#_Toc59520560)

[3.3.2. Đánh giá mức giai đoạn sử dụng tỉ lệ và tỉ lệ phần tram 56](#_Toc59520561)

[3.3.3. Đánh giá mức hoạt động sử dụng cấu trúc phân tích công việc 57](#_Toc59520562)

[Chương IV : Hiện Thực và Đánh Giá Kết Quả 57](#_Toc59520563)

[4.1 Tập Dữ Liệu Thử Nghiệm. 57](#_Toc59520564)

[4.1.1 Tập dữ liệu thử nghiệm 1. 57](#_Toc59520565)

[4.2 Thí Nghiệm và Đánh Giá Kết Quả 63](#_Toc59520566)

[4.2.1 Kết quả của thí nghiệm 1 63](#_Toc59520567)

[4.3. Đánh giá kết quả 66](#_Toc59520568)

[Chương V : Kết Luận 68](#_Toc59520569)

[5.1. Kết luận 68](#_Toc59520570)

[5.2. Ưu - Nhược Điểm 68](#_Toc59520571)

[5.3. Hướng Mở Rộng Tương Lai 68](#_Toc59520572)

[Tài Liệu Tham Khảo 70](#_Toc59520573)

# bảng viết tắt

fdfdMục Lục Bảng

# mục lục hình ảnh

[Hình ảnh. 1Lượt đồ chung cho quá trình giấu tin 18](file:///C:\Users\3IEv3n\Downloads\báo-cáo-đồ-án1%20(1).docx#_Toc59519640)

[Hình ảnh. 2 Lược đồ chung cho quá trình tách tin 19](file:///C:\Users\3IEv3n\Downloads\báo-cáo-đồ-án1%20(1).docx#_Toc59519641)

[Hình ảnh. 3 Sự khác nhau giữa mã hóa và giấu tin 20](file:///C:\Users\3IEv3n\Downloads\báo-cáo-đồ-án1%20(1).docx#_Toc59519642)

[Hình ảnh. 4 Phân loại các kỹ thuật thủy vân 28](file:///C:\Users\3IEv3n\Downloads\báo-cáo-đồ-án1%20(1).docx#_Toc59519643)

[Hình ảnh. 5 Ảnh gốc và năng lượng phân bố của ảnh qua phép biến đổi DCT 31](file:///C:\Users\3IEv3n\Downloads\báo-cáo-đồ-án1%20(1).docx#_Toc59519644)

[Hình ảnh. 6 Phân chia 3 miền tần số ảnh của phép biến đổi DCT 32](#_Toc59519645)

[Hình ảnh. 7 Cấu trúc phân tích và ảnh phân tích được qua phép biến đổi sóng nhỏ 36](#_Toc59519646)

[Hình ảnh. 8 Minh họa thuật toán SW: nhúng bit 1 vào khối ảnh B. 43](file:///C:\Users\3IEv3n\Downloads\báo-cáo-đồ-án1%20(1).docx#_Toc59519647)

[Hình ảnh. 9 Minh họa chọn điểm ảnh giấu tin vào những khối ảnh màu. 44](file:///C:\Users\3IEv3n\Downloads\báo-cáo-đồ-án1%20(1).docx#_Toc59519648)

# Chương I : Giới Thiệu

* 1. Giới Thiệu Nội Dung Đề Tài

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 đổi mới. Với việc sử dụng mạng internet toàn cầu để thông tin, liên lạc ngày càng tăng trong mọi lĩnh vực chính trị, quân sự, quốc phòng, kinh tế và thương mại,…Vấn đề được đặt ra đó là sự an toàn dữ liệu.

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,…

Việc che giấu thông tin trong ứng dụng hay một vật mang tin cụ thể không quá xa lạ đối với các nhà phát triển đang làm việc trong lĩnh vực an toàn thông tin, nhưng với việc che giấu thông tin sử dụng công nghệ thực tế ảo và thực tế ảo tăng cường là một bước tiến mới. Đồng thời việc này có thể chỉ rõ ra rằng, tội phạm công nghệ cao có thể có những đột biến đáng ngờ về phương thức và hành vi phạm tội.

Mục tiêu của việc nghiên cứu thực hiện đồ án tốt nghiệp với đề tài : Nghiên Cứu Cơ Chế Giấu Tin Trong Ảnh và Ứng Dụng Trong Mã hóa Dữ Liệu. Là nhằm tìm hiểu và xây dựng một môi trường giấu tin trong ảnh bằng phương pháp mã hóa dữ liệu. Ngày nay, nhu cầu trao đổi thông tin trên mạng là rất lớn. Theo đó, vấn đề bảo đảm an toàn cho những thông tin mật cũng trở nên cấp thiết. Có nhiều giải pháp nhằm đảm bảo an toàn cho thông tin trao đổi, giấu tin trong ảnh là một giải pháp được nhiều nhà khoa học quan tâm nghiên cứu.

* 1. Mục Tiêu Nội Dung Đề Tài
* **Mục tiêu :** Xây dựng cơ chế giấu tin trong ảnh.
* **Nội dung đề tài :**
* Tìm hiểu cơ chế giấu tin trong ảnh.
* Tìm hiểu các công trình nghiên cứu liên quan và phân tích ưu nhược điểm của chúng.
* Đề suất cơ chế giấu tin trong ảnh.
* Xây dựng ứng dụng giấu tin trong ảnh.
* Đánh giá và so sánh các phương pháp giấu tin trong ảnh.
  1. Giới Hạn Đề Tài
* Nội dung cần làm :
* Nghiên cứu các phương pháp giấu tin trong ảnh.
* Kỹ thuật thủy vân sử dụng phép biến đổi cosin rời rạc.
* Kỹ thuật thủy vân của Shoemarker C.
* Kỹ thuật thủy vân sử dụng phép biến đổi nhỏ Discrete wavelet transform – DWT.
* Kỹ thuật thủy vân của Mehul R. và Priti R
* Kỹ thuật thủy vân của Tao P. và Eskicioglu A.M.
* Thuật toán SW (Simple Watermarking).
* Thuật toán WU-LEE.
* Thuật toán LSB (Least Significant Bits).

Sử dụng phương pháp LSB (Least Significant Bits) thực hiện bằng cách thay đổi các bit ít quan trọng của ảnh 8 bit.

* Hiện thực ứng dụng kỹ thuật giấu tin trong ảnh để mã hóa thông điệp và giấu dữ liệu trong ảnh.
* Thứ nhất có một thông điệp cần giấu trong một file hình ảnh.
* Thứ hai tiến hành mã hóa thông điệp bằng thuật toán AES với khóa AES được sinh ra bằng phần mềm hiện thực.
* Thứ ba tiến hành tạo khóa bí mật bằng khóa bí mật ban đầu và sử dụng thuật toán BIP0032.
* Thứ tư kết hợp kết quả mã hóa thông điệp từ thuật toán AES với khóa bí mật được tạo ra, tiến hành nhúng LSB vào hình ảnh ban đầu.
* Thứ năm kết quả của quá trình nhúng LSB là hình ảnh đã được ẩn giấu thông điệp.

* 1. Cấu Trúc Báo Cáo

Luận văn được tổ chức gồm 5 chương với nội dung chính sau :

* Chương 1 : Giới Thiệu.

Giới thiệu tổng quan về đề tài. Chương này chủ yếu trình bày mục tiêu, nội dung, giới hạn và cấu trúc của báo cáo về đề tài “ Nghiên cứu cơ chế giấu tin trong ảnh và ứng dụng trong mã hóa dữ liệu ”.

* Chương 2 : Cơ sở lý thuyết và các nghiên cứ liên quan

Chương này trình bày tổng quan về cơ chế giấu tin trong ảnh, phân tích, đánh giá từng kỹ thuật liên quan đến cơ chế giấu tin trong ảnh.

* Chương 3 : Phương pháp nghiên cứu cơ chế giấu tin trong ảnh và ứng dụng trong mã hóa dữ liệu.

Chương này giới thiệu về các yêu cầu của bài toán, đề xuất phương pháp áp dụng trong cơ chế giấu tin trong ảnh, đưa ra được các phương pháp đánh giá về đề tài.

* Chương 4 : Hiện thực và đánh giá kết quả

Chương này trình bày hiện thực quá trình đưa thông điệp vào hình ảnh (và thực hiện nhúng thủy vấn) – và tách thủy vân để lấy ra thông điệp ban đầu. Đưa ra kết một số kết quả thực nghiệm

* Chương 5 : Kết luận

Tổng quan đồ án, đánh giá ưu nhược điểm của phương pháp đã chọn, hướng phát triển trong tương lai.

# Chương II : Cơ Sở Lý Thuyết và Các Nghiên Cứu Liên Quan

2.1 Cơ Sở Lý Thuyết

### 2.1.1 Định Nghĩa

* Giấu thông tin (Steganography) là một kỹ thuật nhúng thông tin *(embeding)* vào trong một nguồn đa phương tiện gọi là các phương tiện chứa (host data) mà không gây ra sự nhận biết về sự tồn tại của thông tin giấu *(invisible)*.
* Hay ta cũng có thể định nghĩa tổng quát như sau: Giấu tin là kỹ thuật nhúng một lượng thông tin số nào đó vào trong một đối tượng dữ liệu số khác.

### 2.1.2 Vài nét về lịch sử giấu tin.

* Từ Steganography bắt nguồn từ tiếng Hi Lạp và được sử dụng cho tới ngày nay, nó có nghĩa là tài liệu được phủ (covered writing). Các câu chuyện kể về kỹ thuật giấu thông tin được truyền qua nhiều thế hệ. Có lẽ những ghi chép sớm nhất về kỹ thuật giấu thông tin (thông tin được hiểu theo nghĩa nguyên thủy của nó) thuộc về sử gia Herodotus người Hy lạp. Khi bạo chúa Hy lạp Histiaeus bị vua Darius bắt giữ ở Susa vào thế kỷ thứ năm trước Công nguyên, ông đã gửi một thông báo bí mật cho con rể của mình là Aristagoras ở Miletus. Histiaeus đã cạo trọc đầu của một nô lệ tin cậy và xăm một thông báo trên da đầu của người nô lệ ấy. Khi tóc của người nô lệ này mọc đủ dài, anh ta đã được gửi tới Miletus.
* Một câu chuyện khác ở thời Hy-Lạp cổ đại cũng do Herodotus ghi lại. Môi trường để ghi văn bản chính là các viên thuốc được bọc trong sáp ong. Demeratus, một người Hy lạp, cần thông báo cho Sparta rằng Xerxes định xâm chiếm Hy lạp. Để tránh bị phát hiện, anh ta đã bóc lớp sáp ra khỏi các viên thuốc và khắc thông báo lên bề mặt các viên thuốc này, sau đó bọc lại các viên thuốc bằng một lớp sáp mới. Những viên thuốc được để ngỏ và lọt qua mọi sự kiểm tra một cách dễ dàng.
* Một cách giấu tin phổ biến là sử dụng mực không màu. Đây là một phương tiện hữu hiệu cho bảo mật thông tin trong một thời gian dài. Người Romans cổ đã biết sử dụng những chất sẵn có như nước quả, nước tiểu và sữa để viết các thông báo bí mật giữa những hàng văn tự thông thường. Khi bị hơ nóng, những loại mực không nhìn thấy này sẽ trở nên sẫm màu và có thể đọc được một cách dễ dàng. Mực không màu cũng được sử dụng rất gần đây, như trong thời gian chiến tranh Thế giới lần thứ II.
* Ý tưởng che giấu thông tin đã có từ hàng nghìn năm về trước nhưng kỹ thuật này được dùng chủ yếu trong quân đội và trong các cơ quan tình báo. Mãi cho tới vài thập niên gần đây, giấu thông tin mới được các nhà nghiên cứu và các viện công nghệ thông tin quan tâm và đã có rất nhiều các công trình nghiên cứu về vấn đề này. Cuộc cách mạng số hoá thông tin và sự phát triển nhanh chóng của mạng truyền thông là nguyên nhân chính dẫn đến sự thay đổi này. Những phiên bản sao chép hoàn hảo, các kỹ thuật thay thế, sửa đổi tinh vi, cộng với sự lưu thông phân phối trên mạng của các dữ liệu đa phương tiện đã sinh ra rất nhiều vấn đề nhức nhối về nạn ăn cắp bản quyền, phân phối bất hợp pháp, xuyên tạc trái phép...

### 2.1.3 Mô hình kỹ thuật giấu tin và các thuật ngữ cơ bản

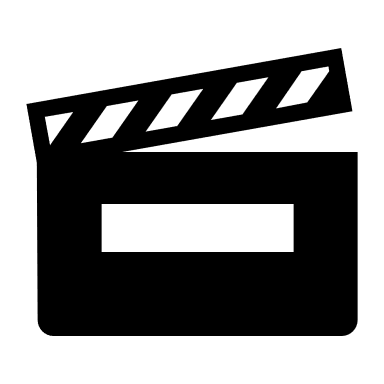
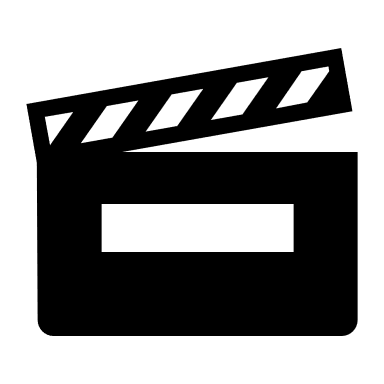
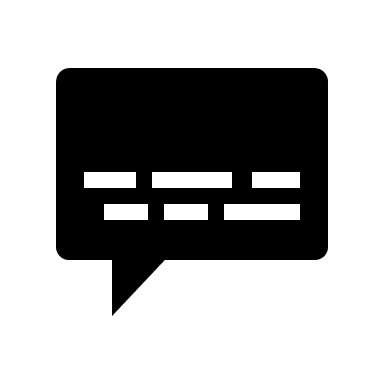
Mô hình của kỹ thuật giấu tin cơ bản được mô tả trong các Hình 1 và 2. Trong đó, Hình 1 biểu diễn quá trình giấu tin cơ bản. Phương tiện chứa bao gồm các đối tượng được dùng làm môi trường để giấu tin như text, audio, video, image …

Thông tin cần giấu là một lượng thông tin mang một ý nghĩa nào đó tuỳ thuộc vào mục đích của người sử dụng. Thông tin sẽ được giấu vào trong một phương tiện chứa nhờ một bộ nhúng. Bộ nhúng là những chương trình, thuật toán giấu tin và được thực hiện với một khoá bí mật giống như các hệ mã mật cổ điển. Sau khi giấu tin, các phương tiện chứa có giấu tin sẽ được gửi đi hoặc được phân phối sử dụng trên mạng.

Thông điệp cần giấu

Bộ nhúng thông tin

Hình ảnh đã được giấu tin



Hình ảnh đầu vào

Hình ảnh

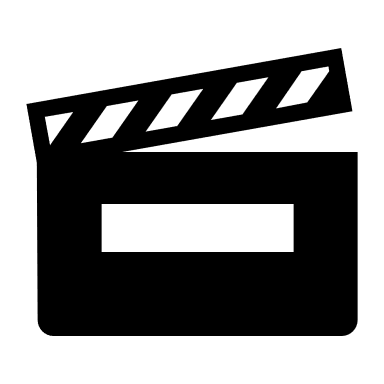
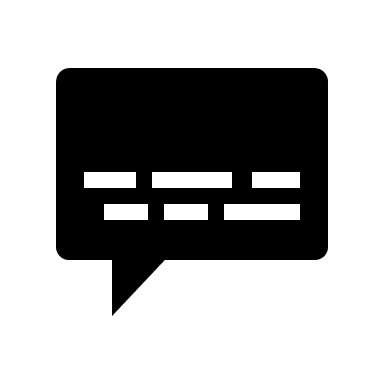
đầu ra

Hình ảnh. Lượt đồ chung cho quá trình giấu tin

Hình 2 chỉ ra các công việc giải mã thông tin đã giấu. Quá trình giải mã được thực hiện thông qua một bộ giải mã tương ứng với bộ nhúng thông tin cùng với khoá của quá trình nhúng. Kết quả thu được gồm phương tiện chứa gốc và thông tin đã giấu. Bước tiếp theo, thông tin giấu sẽ được xử lý, kiểm định so sánh với thông tin giấu ban đầu.

Kiểm định

Hình ảnh đầu ra



Hình ảnh chứa đã được giấu tin

Bộ lọc tin

Thông điệp giấu

Hình ảnh. Lược đồ chung cho quá trình tách tin

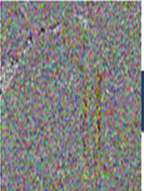
Một số thuật ngữ cơ bản:

* **Giấu tin** (**datahiding**)**:** là thuật ngữ chỉ kỹ thuật giấu tin nói chung bao gồm cả giấu tin mật và thuỷ vân số.
* **Giấu tin mật** (**steganography**)**:** chỉ những kỹ thuật giấu tin mật trong một đối tượng.
* **Thuỷ vân số** (**watermarking**)**:** chỉ những kỹ thuật giấu tin dùng để bảo vệ đối tượng chứa thông tin giấu.
* **Phương tiện chứa** (**host signal**)**:** là phương tiện gốc được dùng để chứa thông tin cần giấu. Nếu giấu tin trong ảnh thì bức ảnh này được gọi là ảnh chứa, còn giấu trong audio thì gọi là audio chứa v.v..
* **Thông tin cần giấu** (**embeded data**)**:** là thông tin được nhúng vào trong phương tiện chứa. Trong giấu tin mật, thông tin cần giấu là các thông điệp (message), còn trong kỹ thuật thuỷ vân số thì thông tin cần giấu chính là các thuỷ vân (các dấu hiệu công khai hoặc bí mật).

### 2.1.4 Sự khác biệt giữa mã hóa và giấu tin.

Sự khác biệt chủ yếu giữa mã hoá thông tin và giấu thông tin là phương pháp mã hoá làm cho các thông tin hiện rõ là nó có được mã hoá hay không còn đối với phương pháp giấu thông tin thì người ta sẽ khó biết được là có thông tin giấu bên trong do tính chất ẩn (invisible) của thông tin được giấu. Một khi những thông tin mã hoá bị phát hiện thì những tên tin tặc sẽ tìm mọi cách ðể triệt phá. Và cuộc chạy ðua giữa những ngýời bảo vệ thông tin và bọn tin tặc vẫn chýa kết thúc tuyệt ðối về bên nào. Trong hoàn cảnh ðó thì giấu thông tin trở thành một phương pháp hữu hiệu.

Sự khác nhau này ta có thể thấy rõ qua hình 3.



Mã Hóa

Giải Mã



Giấu Tin

Giải Tin

Hình ảnh. Sự khác nhau giữa mã hóa và giấu tin

### 2.1.5 Giấu tin trong dữ liệu đa phương tiện

Kỹ thuật giấu tin đã được nghiên cứu và áp dụng trong nhiều môi trường dữ liệu khác nhau trong dữ liệu đa phương tiện (text, image, audio, video), trong sản phẩm phần mềm và gần đây là những nghiên cứu trên môi trường cơ sở dữ liệu quan hệ. Trong các môi trường dữ liệu đó thì dữ liệu đa phương tiện là môi trường chiếm tỉ lệ chủ yếu trong các kỹ thuật giấu tin.

#### 2.1.5.1 Giấu tin trong ảnh

Gấu tin trong ảnh là làm cách nào đó tác động lên ảnh để có thể đưa thông tin cần giấu vào ảnh mà bằng mắt thường con người không thể nhận ra thông tin giấu và cũng không thể nhận biết được sự hiện diện của tin giấu trong ảnh.

Giấu tin trong ảnh sẽ làm cho thông tin không bị bọn tội phạm chú ý và tấn công, điều này tương tự như việc ngụy trang các đoàn xe vận tải trong chiến tranh và ảnh mang tin (Host Image) đóng vai trò như là cành lá ngụy trang.

Việc không gây chú ý đối với bọn tội phạm là lợi thế quan trọng nhất của giấu tin trong ảnh. Giả sử nếu ta gửi cho đối tác một thông điệp quan trọng đã được mã hóa qua Internet và thật không may nó bị rơi vào tay bọn tội phạm, lập tức bọn tội phạm sẽ tiến hành giải mã và tấn công thông tin, điều này làm tăng nguy cơ bị lộ của thông tin cho dù phương pháp mã hóa có tốt đến đâu chăng nữa. Tuy nhiên nếu ta giấu tin vào trong một bức ảnh thì khả năng thông tin bị tấn công sẽ giảm đi rất nhiều vì hàng ngày có rất nhiều bức ảnh qua lại trên Internet và bức ảnh có giấu tin của ta cũng giống như bao bức ảnh khác vì thế nó ít gây chú ý với bọn tội phạm.

Giấu thông tin trong ảnh, hiện nay là một bộ phận chiếm tỉ lệ lớn nhất trong các chương trình ứng dụng, các phần mềm, hệ thống giấu tin trong đa phương tiện bởi lượng thông tin được trao đổi bằng ảnh là rất lớn và hơn nữa giấu thông tin trong ảnh cũng đóng vai trò hết sức quan trọng trong các hầu hết các ứng dụng bảo vệ an toàn thông tin như: nhận thực thông tin, xác định xuyên tạc thông tin, bảo vệ bản quyền tác giả, điều khiển truy cập, giấu thông tin mật...Chính vì thế mà vấn đề này đã nhận được sự quan tâm rất lớn của các cá nhân, các tổ chức, các trường đại học và viện nghiên cứu trên thế giới.

Thông tin sẽ được giấu cùng với dữ liệu ảnh nhưng chất lượng ảnh ít bị thay đổi và ít người có thể biết được đằng sau ảnh đó mang những thông tin có ý nghĩa. Ngày nay, khi ảnh số đã được sử dụng rất phổ biến, thì giấu thông tin trong ảnh đã cung cấp nhiều ứng dụng quan trọng trong rất nhiều lĩnh vực của đời sống xã hội. Ví dụ như đối với các nước phát triển, chữ kí tay đã được số hoá và được lưu trữ trong hồ sơ cá nhân của các dịch vụ ngân hàng và tài chính và được sử dụng để chứng thực như các chữ ký sống. Phần mềm WinWord của MicroSoft 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 an toàn của thông tin. Tài liệu sau đó được truyền trực tiếp qua máy fax hoặc lưu truyền trên mạng. Vì thế, việc nhận thực chữ kí, xác thực thông tin đã trở thành một vấn đề cực kì quan trọng khi mà việc ăn cắp thông tin hay xuyên tạc thông tin bởi các tin tặc đang trở thành một vấn nạn đối với bất kì quốc gia nào, tổ chức nào. Thêm vào đó, lại có rất nhiều loại thông tin quan trọng cần được bảo mật như những thông tin về an ninh, thông tin về bảo hiểm hay các thông tin về tài chính, các thông tin này được số hoá và lưu trữ trong hệ thống máy tính hay trên mạng. Chúng rất dễ bị lấy cắp và bị thay đổi bởi các phần mềm chuyên dụng. Việc nhận thực cũng như phát hiện thông tin xuyên tạc đã trở nên vô cùng quan trọng và cấp thiết. Một đặc điểm của giấu thông tin trong ảnh đó là thông tin được giấu trong ảnh một cách vô hình, nó như là một cách truyền thông tin mật cho nhau mà người khác không thể biết được bởi sau khi giấu thông tin thì chất lượng ảnh gần như không thay đổi, đặc biệt đối với ảnh mầu hay ảnh xám. Trước đây, báo chí đã đưa tin vụ việc ngày 11-9 gây chấn động nước Mỹ và toàn thế giới, chính tên trùm khủng bố quốc tế Osama Bin Laden đã dùng cách thức giấu thông tin trong ảnh để liên lạc với đồng bọn, và đã qua mặt được Cục tình báo trung ương Mỹ CIA và các cơ quan an ninh quốc tế. Chắc chắn sau vụ việc này, việc nghiên cứu các vấn đề liên quan đến giấu thông tin trong ảnh sẽ được quan tâm đặc biệt hơn nữa.

#### 2.1.5.2 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 lại 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). 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 cũng may là HAS lại kém trong việc phát hiện sự khác biệt của các giải 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 lý 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, 44.100Hz) có chiều dài bình thường thì các phương pháp giấu tin nói chung cũng cần ít nhất là 20bps. 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.

#### 2.1.5.3 Giấu tin trong Video

Cũng giống như giấu thông tin trong ảnh hay trong audio, giấu tin trong video cũng được quan tâm và được phát triển mạnh mẽ cho nhiều ứng dụng như kiểm soát sao chép thông tin, nhận thực thông tin và bảo vệ bản quyền tác giả. Ta có thể lấy một ví dụ là các hệ thống chương trình trả tiền xem theo đoạn với các video clip (pay per view application). Các kỹ thuật giấu tin trong video đã được phát triển mạnh mẽ và cũng theo hai khuynh hướng thuỷ vân và giấu tin mật. Trong báo cáo này chỉ quan tâm tới các kỹ thuật giấu tin trong video. Một phương pháp giấu tin trong video do tác giả Cox đề xuất 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 chứa gốc. Nhiều nhà nghiên cứu đã dùng những hàm cosin riêng và các hệ số truyền sóng riêng để giấu tin. Trong các thuật toán sơ khai, người ta chỉ đưa ra các kỹ thuật cho phép giấu ảnh vào trong video nhưng thời gian gần đây các kỹ thuật mới đã cho phép giấu cả âm thanh và hình ảnh vào video. Như phương pháp của Swanson đã sử dụng cách giấu theo khối, phương pháp này đã giấu được hai bit vào khối 8\*8. Hay gần đây nhất là phương pháp của Mukherjee là kỹ thuật giấu audio vào video sử dụng cấu trúc lưới đa chiều...

Nói tóm lại, kỹ thuật giấu thông tin đã thành công nhờ biết tận dụng được những đặc điểm thị giác và thính giác của con người.

Hơn nữa, kỹ thuật giấu tin đang được áp dụng cho nhiều loại đối tượng chứ không chỉ riêng gì cho các dữ liệu đa phương tiện như ảnh, audio hay video. Gần đây, đã có một số nghiên cứu giấu tin trong cơ sở dữ liệu quan hệ và cơ sở dữ liệu XML. Chắc chắn sau này kỹ thuật giấu tin sẽ phát triển tiếp tục và mạnh hơn nữa.

#### 2.1.5.4 Giấu tin trong văn bản

Trong việc trao đổi thông tin qua hệ thống máy tính, văn bản chiếm một tỷ lệ rất lớn so với các loại phương tiện chứa khác. Tuy vậy, giấu tin trong văn bản lại chưa được quan tâm nghiên cứu nhiều. Các nghiên cứu về giấu tin trong văn bản được chia theo hai hướng, thứ nhất văn bản được sử dụng để giấu tin là những văn bản được chụp lại và lưu trên máy như một bức ảnh nhị phân. Theo hướng này, các kỹ thuật giấu tin được thực hiện như kỹ thuật giấu tin trong ảnh. Hướng thứ hai, phương tiện chứa sử dụng cho quá trình giấu tin được lưu dưới dạng văn bản. Theo hướng này, các kỹ thuật giấu tin cũng tiến hành như giấu tin trong ảnh bằng cách thay đổi một số ký tự tại một số vị trí trên văn bản mà không làm ảnh hưởng nhiều đến nội dung văn bản gốc.

#### 2.1.5.5 Giấu tin trong ảnh, những đặc trưng và tính chất.

Giấu tin trong ảnh chiếm vị trí chủ yếu trong các kỹ thuật giấu tin, vì vậy các kỹ thuật giấu tin phần lớn cũng tập trung vào các kỹ thuật giấu tin trong ảnh. Các phương tiện chứa khác nhau thì cũng sẽ có các kỹ thuật giấu khác nhau. Đối tượng ảnh là một đối tượng dữ liệu tĩnh, dữ liệu tri giác không biến đổi theo thời gian. Dữ liệu ảnh có nhiều định dạng, mỗi định dạng có những tính chất khác nhau nên các kỹ thuật giấu tin trong ảnh thường chú ý những đặc trưng và các tính chất cơ bản sau đây:

* *Phương tiện chứa có dữ liệu tri giác tĩnh.* Dữ liệu gốc ở đây là dữ liệu của ảnh tĩnh, dù đã giấu thông tin vào trong ảnh hay chưa thì khi ta xem ảnh bằng thị giác, dữ liệu ảnh không thay đổi theo thời gian, điều này khác với dữ liệu audio hay là video vì khi ta nghe hay xem thì dữ liệu gốc sẽ thay đổi liên tục với tri giác của con người theo các đoạn hay các bài, các cảnh... Sự khác biệt này ảnh hưởng lớn đối với các kỹ thuật giấu thông tin trong ảnh với kỹ thuật giấu thông tin trong audio hay video.
* *Kỹ thuật giấu phụ thuộc ảnh.* Kỹ thuật giấu tin phụ thuộc vào các loại ảnh khác nhau. Chẳng hạn đối với ảnh đen trắng, ảnh đa mức xám hay ảnh màu ta có những kỹ thuật riêng do các loại ảnh có những đặc trưng khác nhau.
* *Kỹ thuật giấu tin lợi dụng tính chất hệ thống thị giác của con người.* Giấu tin trong ảnh ít nhiều cũng gây ra những thay đổi trên dữ liệu ảnh gốc. Dữ liệu ảnh được quan sát bằng hệ thống thị giác của con người nên các kỹ thuật giấu tin phải đảm bảo một yêu cầu cơ bản là những thay đổi trên ảnh phải rất nhỏ sao cho bằng mắt thường khó nhận ra được sự thay đổi đó vì có như thế thì mới đảm bảo được độ an toàn cho thông tin giấu. Rất nhiều các kỹ thuật đã lợi dụng các tính chất của hệ thống thị giác để giấu tin chẳng hạn như mắt người cảm nhận về sự biến đổi độ chói kém hơn sự biến đổi màu, cảm nhận của mắt về màu xanh da trời là kém nhất trong ba màu cơ bản.
* *Giấu thông tin trong ảnh tác động lên dữ liệu ảnh nhưng không thay đổi kích thước ảnh.* Các thuật toán thực hiện công việc giấu thông tin sẽ được thực hiện trên dữ liệu của ảnh. Dữ liệu ảnh bao gồm cả phần header, bảng màu (có thể có) và dữ liệu ảnh. Khi giấu thông tin, các phương pháp giấu đều biến đổi các giá trị của các bit trong dữ liệu ảnh chứ không thêm vào hay bớt đi dữ liệu ảnh. Do vậy mà kích thước ảnh trước hay sau khi giấu thông tin là như nhau.
* *Đảm bảo chất lượng ảnh sau khi giấu tin.* Đây là một yêu cầu quan trọng đối với giấu tin trong ảnh. Sau khi giấu tin bên trong, ảnh phải đảm bảo được yêu cầu không bị biến đổi lớn để có thể bị phát hiện dễ dàng so với ảnh gốc. Yêu cầu này khá đơn giản đối với ảnh màu hoặc ảnh đa mức xám bởi mỗi một điểm ảnh được biểu diễn bởi nhiều bit, và khi ta thay đổi một giá trị nhỏ nào đó thì chất lượng ảnh thay đổi không đáng kể, thông tin giấu khó bị phát hiện. Đối với ảnh đen trắng thì việc giấu thông tin phức tạp hơn nhiều, vì mỗi điểm ảnh chỉ là trắng hoặc đen, và nếu ta biến đổi một bit từ đen thành trắng mà không khéo thì sẽ rất dễ bị phát hiện. Do đó, yêu cầu đối với các thuật toán giấu thông tin trong ảnh màu hay ảnh đa mức xám và giấu thông tin trong ảnh đen trắng là khác nhau. Trong khi đối với ảnh màu thì các thuật toán chú trọng vào việc làm sao giấu được càng nhiều thông tin càng tốt thì các thuật toán áp dụng cho ảnh đen trắng lại tập trung vào việc làm thế nào để thông tin giấu khó bị phát hiện nhất.
* *Đảm bảo chất lượng ảnh sau khi giấu tin.* Đây là một yêu cầu quan trọng đối với giấu tin trong ảnh. Sau khi giấu tin bên trong, ảnh phải đảm bảo được yêu cầu không bị biến đổi lớn để có thể bị phát hiện dễ dàng so với ảnh gốc. Yêu cầu này khá đơn giản đối với ảnh màu hoặc ảnh đa mức xám bởi mỗi một điểm ảnh được biểu diễn bởi nhiều bit, và khi ta thay đổi một giá trị nhỏ nào đó thì chất lượng ảnh thay đổi không đáng kể, thông tin giấu khó bị phát hiện. Đối với ảnh đen trắng thì việc giấu thông tin phức tạp hơn nhiều, vì mỗi điểm ảnh chỉ là trắng hoặc đen, và nếu ta biến đổi một bit từ đen thành trắng mà không khéo thì sẽ rất dễ bị phát hiện. Do đó, yêu cầu đối với các thuật toán giấu thông tin trong ảnh màu hay ảnh đa mức xám và giấu thông tin trong ảnh đen trắng là khác nhau. Trong khi đối với ảnh màu thì các thuật toán chú trọng vào việc làm sao giấu được càng nhiều thông tin càng tốt thì các thuật toán áp dụng cho ảnh đen trắng lại tập trung vào việc làm thế nào để thông tin giấu khó bị phát hiện nhất.
* *Vai trò của ảnh gốc khi giải tin.* Các kỹ thuật giấu tin phải xác định rõ ràng quá trình lọc ảnh để lấy thông tin giấu cần đến ảnh gốc hay không. Đa số các kỹ thuật giấu tin mật thường không cần ảnh gốc khi lọc tìm thông tin đã giấu. Thông tin được giấu trong ảnh sẽ được mang cùng với dữ liệu ảnh, khi tách tin chỉ cần ảnh đã mang thông tin giấu mà không cần dùng đến ảnh gốc để so sánh đối chiếu.

#### 2.1.5.6 Giấu tin và thủy vân số

* Tính năng an toàn và bảo mật thông tin của kỹ thuật giấu tin được thể hiện ở hai khía cạnh. Một là bảo vệ cho dữ liệu đem giấu và hai là bảo vệ cho chính đối tượng được sử dụng để giấu tin. Tương ứng với hai khía cạnh đó chúng ta có hai khuynh hướng kỹ thuật rõ ràng đó là giấu tin mật (steganography) và thuỷ vân số (watermarking). Từ “thuỷ vân” có xuất xứ từ kỹ thuật đánh dấu nước thời xưa. Kỹ thuật này là kỹ thuật đánh dấu chìm một hình ảnh logo nào đó lên trên giấy nhằm mục đích trang trí và phân biệt được xuất xứ của sản phẩm giấy.
* Trong kỹ thuật giấu tin mật, thông tin cần giấu được gọi là thông điệp (message) còn trong kỹ thuật thuỷ vân số thì được gọi là thuỷ vân (watermark). Thuỷ vân có thể là một chuỗi các kí tự, hay một hình ảnh, logo nào đó.
* Nói đến thuỷ vân số là nói đến kỹ thuật giấu tin hướng đến những ứng dụng bảo đảm an toàn dữ liệu cho đối tượng được sử dụng để giấu tin như: bảo vệ bản quyền, phát hiện xuyên tạc, nhận thực thông tin, điều khiển sao chép v.v…Có thể thấy rõ là phần ứng dụng của thủy vân rất lớn, mỗi ứng dụng lại có những yêu cầu riêng và tính chất riêng, do đó các kỹ thuật thuỷ vân cũng có những tính năng khác biệt tương ứng:

Thuỷ vân

dễ vỡ

Thuỷ vân ẩn

Thuỷ vân hiện

Thuỷ vân ẩn

Thuỷ vân hiện

Thuỷ vân số

Thuỷ vân

bền vững

Hình ảnh. Phân loại các kỹ thuật thủy vân

* Các kỹ thuật thuỷ vân trên hình 1.5 được phân biệt nhau bởi những đặc trưng, tính chất của từng kỹ thuật và ứng dụng những kỹ thuật đó. Thuỷ vân “dễ vỡ” (fragile) là kỹ thuật nhúng thuỷ vân vào trong ảnh sao cho khi phân phối sản phẩm trong môi trường mở nếu có bất cứ một phép biến đổi nào làm thay đổi đối tượng sản phẩm gốc thì thuỷ vân đã được giấu trong đối tượng sẽ không còn nguyên vẹn như trước khi giấu nữa (dễ vỡ). Các kỹ thuật thuỷ vân có tính chất này được sử dụng trong các ứng dụng nhận thực thông tin (authentication) và phát hiện xuyên tạc thông tin (tamper detection). Rất dễ hiểu vì sao những ứng dụng này cần đến kỹ thuật thuỷ vân dễ vỡ. Ví dụ như để bảo vệ chống xuyên tạc một ảnh nào đó ta nhúng một thuỷ vân vào trong ảnh và sau đó phân phối, quảng bá ảnh đó. Khi cần kiểm tra lại ảnh ta sử dụng hệ thống đọc thủy vân. Nếu không đọc được thuỷ vân hoặc thuỷ vân đã bị sai lệch nhiều so với thuỷ vân ban đầu đã nhúng vào ảnh thì có nghĩa là có thể ảnh đó đã bị thay đổi. Cái khó ở đây là ta phải phân biệt giữa sai lệch thuỷ vân do xuyên tạc và sai lệch do lỗi đường truyền. Ngược lại, với kỹ thuật thuỷ vân dễ vỡ là kỹ thuật thuỷ vân bền vững (robust). Các kỹ thuật thuỷ vân bền vững thường được ứng dụng trong các ứng dụng bảo vệ bản quyền. Trong những ứng dụng đó, thuỷ vân đóng vai trò là thông tin sở hữu của người chủ hợp pháp. Thuỷ vân được nhúng trong sản phẩm như một hình thức dán tem bản quyền. Trong trường hợp như thế, thuỷ vân phải tồn tại bền vững cùng với sản phẩm nhằm chống việc tẩy xoá, làm giả hay biến đổi phá huỷ thuỷ vân. Một yêu cầu lí tưởng đối với thuỷ vân bền vững là nếu muốn loại bỏ thuỷ vân thì chỉ có một cách duy nhất là phá huỷ sản phẩm.
* Thuỷ vân bền vững lại được chia thành hai loại là thuỷ vân ẩn và thuỷ vân hiện. Thuỷ vân hiện là loại thuỷ vân được hiện ngay trên sản phẩm và người dùng có thể nhìn thấy được giống như các biểu tượng kênh chương trình vô tuyến mà chúng ta thường thấy VTV3, CCTV, TV5…Các thuỷ vân hiện trên ảnh thường dưới dạng chìm, mờ hoặc trong suốt để không gây ảnh hưởng đến chất lượng ảnh gốc. Đối với thuỷ vân hiện, thông tin bản quyền hiển thị ngay trên sản phẩm.

2.2. Các Nghiên Cứu Liên Quan

### 2.2.1. Kỹ thuật thuỷ vân sử dụng phép biến đổi cosin rời rạc

#### 2.2.1.1. Phép biến đổi Cosin rời rạc.

Biến đổi Cosin rời rạc viết tắt là DCT (Discrete Cosine Transform) do Ahmed và các đồng nghiệp của ông đưa ra vào năm 1974. Từ đó cho đến nay, nó được sử dụng rất phổ biến trong nhiều kỹ thuật xử lí ảnh số. Trong các kỹ thuật thuỷ vân ảnh dựa trên phép biến đổi dữ liệu ảnh sang miền tần số thì phép biến đổi DCT được sử dụng nhiều nhất.

Trong lĩnh vực xử lý ảnh số ta sử dụng biến đổi DCT 2 chiều có dạng như sau:



Với: Yij là giá trị tại vị trí hàng i, cột j của ma trận DCT.

Xuv Là giá trị tại hàng u, cột v của ma trận ảnh gốc X.

M,N là kích thước của ảnh gốc (M hàng, N cột).





Và biến đổi ngược của nó là:



**Đặc điểm của phép biến đổi DCT trên ảnh hai chiều**

Biến đổi DCT trên ảnh thể hiện đặc tính nội dung về tần số của thông tin ảnh. Hệ số góc trên là lớn và đặc trưng cho giá trị trung bình thành phần một chiều gọi là hệ số DC, còn các hệ số khác có giá trị nhỏ hơn biểu diễn cho các thành phần tần số cao theo hướng ngang và theo hướng thẳng đứng gọi là các hệ số AC.



Hình ảnh. Ảnh gốc và năng lượng phân bố của ảnh qua phép biến đổi DCT

* Bản thân biến đổi DCT không nén được dữ liệu.
* Theo nguyên lý chung, khi biến đổi chi tiết giữa các điểm ảnh càng lớn theo một hướng nào đó trong khối các điểm ảnh, hướng ngang, hướng thẳng đứng hay theo đường chéo, thì tương ứng theo các hướng đó, các hệ số biến đổi DCT cũng lớn.

Tóm lại, DCT làm giảm độ tương quan không gian của thông tin trong khối ảnh. Điều đó cho phép biểu diễn thích hợp ở miền DCT do các hệ số DCT có xu hướng có phần dư thừa ít hơn.

Khối hệ số DCT có thể chia thành 3 miền, miền tần số thấp chứa các thông tin quan trọng ảnh hưởng đến tri giác, miền tần số giữa, và miền tần số cao. Các thông tin trong miền tần số cao thường mang tính tri giác thấp.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | (a) |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  | (b) |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  | (c) |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

Hình ảnh. Phân chia 3 miền tần số ảnh của phép biến đổi DCT

*(a) Miền tần số thấp, (b) Miền tần số ở giữa, (c) Miền tần số cao*

Trong các thuật toán thuỷ vân, miền hệ số DCT tần số cao thường không được sử dụng do nó thường không bền vững với các phép xử lí ảnh, hoặc nén ảnh JPEG. Miền tần số thấp cũng ít được sử dụng do một sự thay đổi dù nhỏ trong miền này cũng làm giảm chất lượng tri giác của ảnh. Vì vậy, miền tần số ở giữa thường hay được sử dụng nhất và cũng cho kết quả tốt nhất.

### 2.1.2 Kỹ thuật thủy vân của Shoemarker C.

Shoemarker C. đã sử dụng phép biến đổi DCT để phân tích khối được chọn từ ảnh gốc thành các miền tần số, rồi chọn một cặp 2 hệ số trong miền tần số giữa để thực hiện quá trình nhúng một bit thuỷ vân. Quá trình nhúng luôn đảm bảo sau khi nhúng bit thuỷ vân thì khoảng cách về giá trị giữa hai hệ số được chọn có giá trị lớn hơn hoặc bằng k cho trước.

#### 2.2.1.2.1. Quá trình nhúng thủy vân

* InPut :
* Thủy vân : Một chuỗi các bit S hoặc một ảnh nhị phân W.
* Một ảnh gốc F.
* OutPut
* Ảnh đã nhúng thuỷ vân *Fw*.
* Thực hiện :

1. Ảnh gốc có kích thước m×n sẽ được chia thành (m×n)/64 khối 8×8, mỗi bit của thuỷ vân sẽ được nhúng trong một khối.
2. Chọn một khối ảnh gốc *F*i(8×8), thực hiện phép biến đổi DCT với *F*i để được .
3. Chọn hai hệ số thuộc miền tần số giữa của , giả sử đó là (u,v) và (p,q), đọc bit thuỷ vân cần nhúng giả sử đó là bi.
4. Nếu bít cần nhúng bi=0 và nếu (u,v)< (p,q) thì đổi chỗ hai hệ số này. Ngược lại nếu bít cần nhúng bi=1 và nếu (u,v)≥ (p,q) thì đổi chỗ hai hệ số này.
5. Nếu (u,v)> (p,q) và nếu (u,v)- (p,q)<k thì tăng (u,v) đồng thời giảm (p,q) k/2. Ngược lại, nếu (u,v)≤ (p,q) và (p,q)- (u,v)<k thì tăng (p,q) đồng thời giảm (u,v) k/2.
6. Dùng phép biến đổi ngược IDCT với mỗi khối đã nhúng thuỷ vân .
7. Ghép các khối ảnh để được ảnh đã nhúng thuỷ vân *Fw*.

#### 2.2.1.2.2 Quá trình tách thủy vân

* InPut:
* Ảnh chứa thủy vân Fw.
* Output:
* Thủy vân W tách được từ ảnh Fw.
* Thực hiện:
* Chia Fw thành các khối 8×8.
* Lần lượt chọn các khối 8×8 rồi biến đổi DCT để được 
* Đọc vào vị trí hai hệ số đã biến đổi (u,v) và (p,q) tương ứng với 
* Tính: *k* = (u,v) – (p,q)
* Nếu k > 0 thì gán bi = 0, ngược lại gán bi = 1.
* Ghép dãy bit bi để được ảnh thuỷ vân *W*.

Cách chọn hệ số trong miền tần số giữa các phép biến đổi DCT của Shoemarker C. có những hạn chế:

* Thứ nhất, nếu chọn cố định cặp hệ số thì việc dò tìm và gỡ bỏ thuỷ vân của những người sử dụng ảnh bất hợp pháp là khá dễ dàng và do đó hệ thống không đảm bảo an toàn cho thuỷ vân.
* Thứ hai, trong cả hai cách chọn đều dẫn đến khả năng phải biến đổi cặp hệ số đã chọn cho phù hợp với điều kiện nhúng bit thuỷ vân tương ứng. Thao tác này dẫn đến chất lượng ảnh sau khi nhúng thuỷ vân bị ảnh hưởng đáng kể.

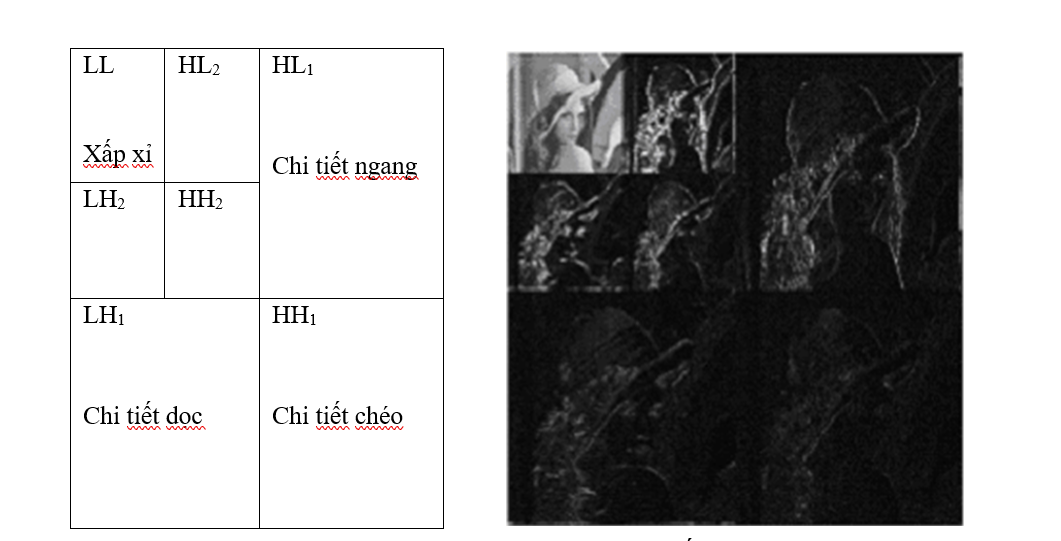
Để khắc phục các nhược điểm nêu trên, trong [3] tác giả đã tiến hành xác định các cặp hệ số trong miền tần số giữa đã thoả mãn điều kiện nhúng bit thuỷ vân, việc biến đổi cặp hệ số chỉ diễn ra khi trong khối không có cặp hệ số nào thoả mãn, điều này làm giảm đáng kể sự thay đổi các giá trị điểm ảnh. Hơn nữa, trong số các cặp hệ số đã tìm được thoả mãn điều kiện giấu, phương pháp chọn ngẫu nhiên cho từng khối làm tăng tính bí mật của thuỷ vân trong ảnh, việc phát hiện thuỷ vân khi không biết thông tin khoá trở lên khó khăn hơn.

### 2.2.2 Một số kỹ thuật thủy vân sử dụng phép biến đổi sóng nhỏ

#### 2.2.2.1 Phép biến đổi sóng nhỏ (DWT)

Ý tưởng của phép biến đổi sóng nhỏ (Discrete wavelet transform - DWT) cho tín hiệu một chiều như sau: Tín hiệu được chia thành 2 phần, phần tần số cao và phần tần số thấp. Thành phần tần số thấp lại được chia tiếp thành hai phần có tần số cao và thấp. Với các bài toán nén và thuỷ vân thường áp dụng không quá năm lần bước phân chia trên. Ngoài ra, từ các hệ số DWT, ta có thể tạo lại ảnh ban đầu bằng quá trình DWT ngược hay IDWT.

Trong hình 2.3, sau 2 lần thực hiện phép biến đổi DWT, ta thu được bảy băng tần con. Các tần số thấp (đạt được bằng lọc thông thấp liên tiếp) tập trung ở góc trái trên và trông giống như một ảnh thu nhỏ của ảnh gốc, vì vậy dải phụ này còn được gọi là băng tần xấp xỉ. Các thành phần tần số cao của ảnh ở trong các băng tần chi tiết còn lại.



Hình ảnh. Cấu trúc phân tích và ảnh phân tích được qua phép biến đổi sóng nhỏ

hai chiều mức 2.

Biến đổi sóng có rất nhiều lợi thế so với các biến đổi khác, đó là:

1. Biến đổi sóng là một mô tả đa độ phân giải của ảnh. Quá trình giải mã có thể được xử lý tuần tự từ độ phân giải thấp cho đến độ phân giải cao.
2. Biến đổi DWT gần gũi với hệ thống thị giác người hơn biến đổi DCT. Vì vậy, có thể nén với tỉ lệ cao bằng DWT mà sự biến đổi ảnh khó nhận thấy hơn nếu dùng DCT với tỉ lệ tương tự.

### 2.2.3 Kỹ thuật thuỷ vân của Mehul R. và Priti R.

Trong kỹ thuật thuỷ vân của Mehul R. và Priti R., các tác giả đã sử dụng phép biến đổi sóng nhỏ hai chiều để phân tích ảnh gốc thành bốn băng LL, HL, LH và HH rồi nhúng tín hiệu thuỷ vân thứ nhất vào băng LL, nhúng một thuỷ vân khác vào băng HH. Kết quả thử nghiệm cho thấy thuỷ vân bền vững trước một số phép xử lý ảnh thông thường.

#### 2.2.3.1. Quá trình nhúng thủy vân.

* InPut:
* Thuỷ vân: hai ảnh nhị phân *J*, *K* kích thước N×N.
* Một ảnh chứa *I* kích thước 4N×4N.
* OutPut:
* Ảnh chứa đã nhúng thuỷ vân *I*’.
* Thực hiện:

1. Sử dụng phép biến đổi song nhỏ hai chiều mức hai đối với *I.*
2. Nhúng thuỷ vân *J* vào băng LL2, nhúng thuỷ vân *K* vào băng HH2 bởi công thức: *V*’i,j = *V*i,j + α*W*i,j. Với *V*i,j là hệ số tương ứng trong LL2 và HH2; α là hệ số tương quan giữa tính ẩn và tính bền vững của thuỷ vân.
3. Sử dụng phép biến đổi ngược IDWT để tổng hợp lại được ảnh chứa thuỷ vân.

#### 2.2.3.2. Quá trình tách thủy vân

* InPut:
* Ảnh gốc *I* và ảnh chứa thuỷ vân *I*’.
* Hệ số tương quan α đã sử dụng khi nhúng thuỷ vân.
* OutPut:
* Ảnh thuỷ vân.
* Thực hiện:

1. Sử dụng phép biến đổi song nhỏ hai chiều mức hai đối với ảnh gốc *I* và ảnh chứa thủy vân *I*’.
2. Từ kết quả phân tích trên, tính giá trị lệch giữa các điểm tương ứng thuộc các băng LL2, HH2 của ảnh chứa thuỷ vân và ảnh gốc rồi chia cho α để được bit tương ứng thuộc ảnh thuỷ vân:

*W*’i,j = (*V*’i,j – *V*i,j)/α

#### Đánh giá kết quả

Qua thử nghiệm, kỹ thuật thuỷ vân của Mehul R. và Priti R. cho kết quả thuỷ vân bền vững trước một nhóm các biến đổi thông thường đối với ảnh chứa thuỷ vân. Thuỷ vân nhúng ở băng LL bền vững trước một nhóm các phép biến đổi, trong khi thuỷ vân nhúng ở băng HH lại bền vững trước một nhóm các biến đổi khác. Điều đó thể hiện, thuỷ vân được nhúng ở các băng khác nhau thể hiện tính bền vững khác nhau trước các tấn công vào hệ thuỷ vân. Như vậy, có thể sử dụng thuỷ vân nhúng vào tất cả các băng trong phép phân tích sóng nhỏ để có thể tìm được sự bền vững ở ít nhất một trong các băng trước các tấn công hoặc có thể xây dựng một phương pháp nhúng kết hợp vào các băng để tìm một thuỷ vân tổng hợp từ các băng đã nhúng.

Quá trình tách thuỷ vân ở đây được yêu cầu sử dụng cả ảnh gốc và ảnh chứa thuỷ vân.

### Kỹ thuật thuỷ vân của Tao P. và Eskicioglu A. M.

Trong kỹ thuật thuỷ vân của Tao P. và Eskicioglu A.M., các tác giả đã tổng hợp từ một số ý tưởng đã được đề xuất trong một số bài báo trước đó. Từ việc sử dụng phép biến đổi sóng nhỏ hai chiều để phân tích ảnh gốc thành các băng tần khác nhau, rồi nhúng tín hiệu thuỷ vân vào một hoặc một số các băng tần. Theo cách đó, thuỷ vân có thể bền vững trước một số tấn công nhưng lại kém bền vững với một nhóm các tấn công khác. Khắc phục nhược điểm trên, trong thuật toán, các tác giả đã nhúng tín hiệu thuỷ vân vào cả bốn băng tần trong phép phân tích sóng nhỏ, mỗi băng tần có thể sử dụng các hệ số khác nhau [12]. Qua thử nghiệm cho thấy, trước hầu hết các phép biến đổi với ảnh chứa thuỷ vân, luôn tìm và tách ra được thuỷ vân ở ít nhất một băng tần có độ sai khác thấp so với thuỷ vân gốc.

#### 2.2.4.1. Quá trình nhúng thủy vân.

* InPut:
* Ảnh chứa *I* = (*aij*, 0≤*i*, *j*≤*2n*)
* Ảnh thuỷ vân là ảnh nhị phân, *W* = (*wij*∈{0, 1}, 0≤*i*, *j*≤*n*).
* OutPut:
* Ảnh chứa đã được nhúng thủy vân *Iw*.
* Thực hiện:

1. Thực hiện phép biến đổi sóng nhỏ DWT mức một phân tích ảnh chứa *I*.
2. Sửa các miền tần số Vij tương ứng với các băng LL, HL, LH, và HH:  
   
3. Thực hiện phép biến đổi ngược IDWT đối với các băng đã sửa đổi tương ứng trong bước 2 để được ảnh đã nhúng thuỷ vân *Iw*.

#### 2.2.4.2. Quá trình tách thủy vân.

* InPut:
* Ảnh chứa đã nhúng thuỷ vân .
* Ảnh gốc *I*.
* OutPut:
* Thuỷ vân là ảnh nhị phân *W\**.
* Thực hiện:

1. Thực hiện phép biến đổi sóng nhỏ DWT mức một để phân tích ảnh gốc *I* và ảnh đã nhúng thuỷ vân (có thể đã qua xử lý) .
2. Tách thuỷ vân từ các băng LL, HL, LH, và HH:
3. Nếu > 0.5 thì lấy = 1 ngược lại lấy = 0.

#### Đánh giá kết quả

Kết quả thử nghiệm thể hiện: Việc xác định hệ số khác nhau cho mỗi băng tần phụ thuộc vào độ lớn của các hệ số phép biến đổi sóng nhỏ. Trong thử nghiệm, sử dụng hệ số là 8 cho băng LL, hệ số là 2 cho các băng HL, LH và HH. Vấn đề chọn các hệ số dựa trên những cơ sở nào cũng cần được tiếp tục nghiên cứu để có thể đưa ra cơ sở khoa học cho việc lựa chọn các hệ số phù hợp cho từng bức ảnh gốc và thuỷ vân cụ thể.

Đa số các lược đồ thuỷ vân sử dụng phép biến đổi sóng nhỏ thì băng LL chưa được sửa đổi, vì điều đó gây lo ngại về chất lượng thương mại của ảnh sau khi nhúng thuỷ vân. Trong cách tiếp cận này, tuy thuỷ vân được nhúng vào cả bốn băng nhưng giá trị PSNR cho thấy chất lượng thương mại của ảnh sau khi nhúng thuỷ vân là chấp nhận được.

Thuỷ vân được nhúng ở băng tần số thấp thì bền vững đối với một nhóm các tấn công, trong khi thuỷ vân được nhúng ở băng tần số cao lại bền vững trước một nhóm các tấn công khác, thuỷ vân nhúng trong những băng tần số giữa cũng bền vững với một số tấn công. Trong tất cả các tấn công đã thử nghiệm, luôn tách lại được thuỷ vân ít nhất ở một trong các băng với sự chênh lệch thấp so với thuỷ vân gốc.

Có thể đánh giá chất lượng của thuỷ vân tách được bằng cách nhìn trực quan hoặc thông qua kết quả tính toán độ lệch SR.

Trong thử nghiệm, luận văn đã chọn cố định các hệ số cho các băng là 8 và 2. Với các hệ số này, ảnh chứa sau khi nhúng thuỷ vân có chất lượng tốt. Tuy nhiên, khi triển khai, đối với mỗi ảnh chứa cụ thể, có thể tính toán để chọn các hệ số tối ưu cho mỗi băng để cho kết quả là thuỷ vân bền vững nhất qua các tấn công.

Việc thực hiện nhúng thuỷ vân theo thuật toán trên áp dụng phép biến đổi sóng nhỏ mức hai cũng đã được thử nghiệm. Trong trường hợp này, giá trị α được chọn là 20 cho băng LL và 3 cho các băng còn lại. Kết quả thử nghiệm cũng cho những kết luận tương tự như sử dụng phép biến đổi mức một.

### Thuật toán SW (Simple Watermarking).

Đây là một thuật toán đơn giản. Cho một file ảnh Bitmap đen trắng F, dữ liệu thủy vân d được biểu diễn dưới dạng nhị phân (dãy bit 0/1). Các bit 1 gọi là điểm đen, các bit 0 gọi là điểm trắng.

Ý tưởng cơ bản của thuật toán này là chia một ảnh gốc thành các khối nhỏ, trong mỗi khối nhỏ sẽ giấu không quá một bit thông tin.

#### 2.2.5.1. Quá trình nhúng thủy vân.

* Chia F thành các khối kích thước M×N.
* Với mỗi khối B trong F ta xét khả năng giấu một bit dữ liệu di của d theo các bước :
* A
* Bước 1: Tính tổng SUM[B] các điểm đen trong khối B, đặt t = SUM[B] mod 2.
* Bước 2: So sánh tính chẵn lẻ giữa t và di

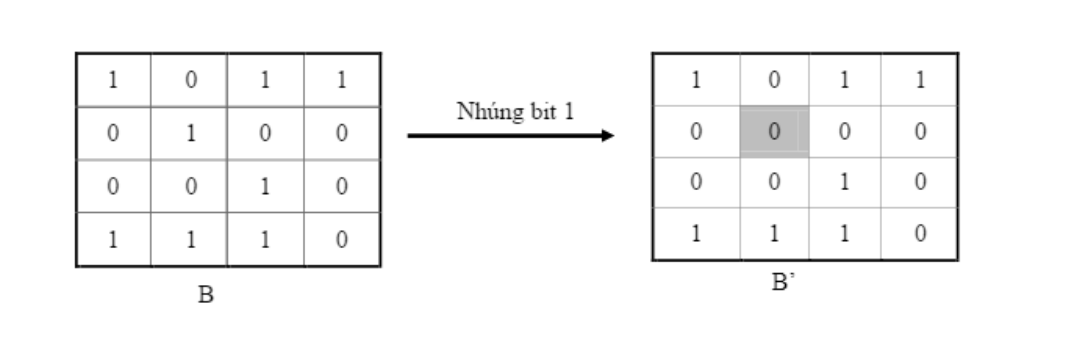
Nếu t và di cùng tính chẵn lẻ thì khối B mặc nhiên đã giấu được bit di mà không cần làm gì.

Nếu t và di khác tính chẵn lẻ thì ta sẽ đảo 1 bit trong B. Chính sách đảo bit: nếu số điểm đen và điểm trắng xấp xỉ nhau thì chọn ngẩu nhiên 1 bit để đảo. Nếu có nhiều điểm đen và có điểm trắng thì sửa điểm trắng thành điểm đen. Ngược lại sẽ sửa điểm đen thành điểm trắng.

Ví dụ minh họa:

Giả sử giấu một bit dữ liệu b = 1 vào khối B.

Ta có SUM (B) = 8. Do SUM (B) mod 2 = 0 nên khối B không thõa mãn yêu cầu để giấu bit 1. Muốn giấu bit 1 vào khối này ta cần phải thay đổi khối bằng cách chọn một bit bất kỳ và đổi từ 0 sang 1 và từ 1 sang 0. Giả sử ta đảo lại bit tại vị trí B [2,2] ta được khối B đã đƣợc nhúng bít 1.



Hình ảnh. Minh họa thuật toán SW: nhúng bit 1 vào khối ảnh B.

Giả sử vẫn với khối B đã cho như trên nhưng ta phải giấu bit dữ liệu b= 0 và khối đó. Ta thấy do Sum (B) = 8 nên

Sum (B) mod 2 = 0. Khối B đƣợc bảo toàn và bit dữ liệu

b = 0 xem như được giấu.

#### 2.2.5.2. Quá trình tách thủy vân.

Trong thuật toán thủy vân này, khóa đơn giản là kích thƣớc của khối,

tức là bộ số (m, n). Nếu biết kích thước của khối thì dễ dàng trích lại dữ liệu d

theo các bước:

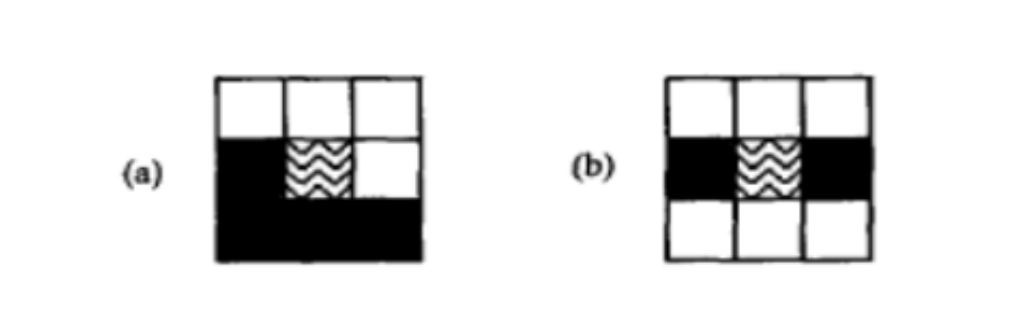
* Bước 1: Chia ảnh có nhúng thủy vân B‟ thành các khối có kích thước

M×N.với mỗi khối Bi‟ trong B‟ ta tính Sum [Bi‟]

* Bước 2: tách thủy vân theo cách xét:
* Nếu Sum [Bi’] là chẵn thì bit di = 0.
* Ngược lại , nếu Sum [Bi’] là lẻ thì bit di = 1

#### Nhận xét.

* Với thuật toán này việc chọn khối khá là đơn giản: ta có thể bắt đầu từ khối đầu tiên và các khối tiếp theo một cách tuần tự. Tuy nhiên, ta có thể chọn ngẫu nhiên một khối chưa giấu ở mỗi lần giấu, hoặc chọn các khối theo một 21 thuật toán xác định kèm theo một khóa K. Khi đó, ta đã làm tăng được độ an toàn của thuật toán vì khóa bây giờ còn thêm cả chỉ số khối đã giấu tin cho từng bit. Hoặc ta có thể thay đổi kích thƣớc khối mỗi lần giấu, chẳng hạn nhƣ khối thứ nhất có kích thƣớc là 8 x 8 thì khối thứ 2 có kích thƣớc 8x12 trong trường hợp này khóa sẽ gồm cả kích thước khối của mỗi lần giấu.
* Kỹ thuật trên sẽ gặp phải hiện tượng gây bất thường đối với ảnh sau khi giấu thông tin đặc biệt khi chọn vào những khối ảnh một màu, chẳng hạn như một khối màu đen hoặc toàn trắng. Khi đó, nếu cần đảo giá trị một bit thì vị trí bit đảo sẽ khác biệt hoàn toàn với các bit trong khối và dễ nhận biết có sự thay đổi. Vì vậy, để xác định nên thay đổi bit nào khối bit ta phải tính hệ số ảnh hƣởng của bit đó khi nó bị thay đổi. Hệ số này tính bằng cách xét sự thay đổi về tính trơn và tính liên kết với các điểm láng giềng. Tính trơn đƣợc đo theo sự chuyển đổi mức xám theo chiều ngang và chiều dọc, đường chéo trong cửa sổ 3x 3. Tính liên kết được tính bằng số nhóm điểm đen và số điểm trắng. Ví dụ: Nếu đảo một điểm ảnh trong hình (a) sẽ ít bị chú ý hơn điểm ảnh trong hình.



Hình ảnh. Minh họa chọn điểm ảnh giấu tin vào những khối ảnh màu.

### Thuật toán WU-LEE

Thuật toán này của hai tác giả M.Y. WU và J.H. Lee đưa ra cải tiến hơn thuật toán 1 bằng việc đưa thêm khóa K sử dụng trong quá trình nhúng và tách thủy vân đồng thời đƣa thêm các điều kiện đảo bit trong mỗi khối. Với thuật toán này, có thể nhúng một bit và mỗi khối bằng cách hiệu chỉnh nhiều nhất 1 bit của khối. Kỹ thuật này có khả năng làm tăng dữ liệu có thể nhúng. 22 Xét ảnh gốc F , khóa bí mật K và một số dữ liệu được nhúng vào F. Khóa bí mật K là một ma trận ảnh có kích thước M×N. Để đơn giản ta giả sử kích thước của ảnh gốc F là bội số của M×N. Quá trình nhúng thu được ảnh F có một số bit đã bị hiệu chỉnh. Thuật toán thực hiện như sau:

#### 2.2.6.1. Quá trình nhúng thủy vân.

* Bước 1 : Chia F thành các khối, mỗi khối có kích thƣớc M×N.
* Bước 2: Với mỗi khối Fi thu được ở bước 1. Kiểm tra điều kiện:

0 < SUM (Fi ^ K) < SUM (K)

Nếu điều kiện trên đúng thì tiếp tục thực hiện bước 3 để nhúng một bit vào Fi . Ngược lại, dữ liệu sẽ không được nhúng vào Fi và Fi sẽ được giữ nguyên.

* Bước 3: Giả sử bit được nhúng vào Fi là b. Được hiệu chỉnh Fi ta làm như sau:
* Trường hợp 1: Nếu SUM (Fi ^ K) mod 2 = b thì không thay đổi Fi và bit b hiện nhiên được nhúng vào khối Fi .
* Trường hợp 2: Nếu SUM (Fi ^ K) mod 2 # b và SUM (Fi ^ K) = 1 thì chọn ngẫu nhiên một bit của Fi tại vị trí (i,j) mà Fi (j,k)=0 và

K (j,k)=1 và đảo Fi (j,k) thành 1.

* Trường hợp 3: Nếu SUM (Fi ^ K) mod 2 # b và SUM (Fi ^ K) = SUM (K) – 1 thì chọn ngẫu nhiên một bit của Fi tại vị trí (j,k) mà K (j,k)=1 và đảo ngược Fi (j,k) thành 0.
* Trường hợp 4: Nếu SUM (Fi ^ K) mod 2 # b và 1< SUM (Fi ^ K) < SUM (K) – 1 thì chọn ngẫu nhiên một bit của Fi tại vị trí (j,k) mà K (j,k)=1 và đảo ngược Fi (j,k).

Trong bước 3 chỉ thực hiện tối đa một phép đảo một bit của Fi để thu được khối Fi’ nhằm đảm bảo tính bất biến.

Ví dụ minh họa: Giả sử ta cần nhúng dãy bit d = 011 và một ảnh F có kích thước 6×6 với một ma trận khóa K có kích thước 3×3 như trong hình. Ta có Sum (K) = 5 23 Chia ảnh F thành bốn khối nhỏ mỗi khối sẽ có kích thước là 3×3 ta thu được F1 , F2, F3, F4 .

Sơ đồ minh họa thuật toán WU-LEE nhúng đoạn bit 01

Áp dụng thuật toán, lần lượt nhúng các bit vào các khối như sau:

* Với F1, Vì SUM (F1 ^ K) = 5 = SUM (K) không thỏa mãn điều kiện nhúng nên không nhúng dữ liệu vào trong F1.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 11 |  |  | F2 |  |
| 1 | 1 | 0 | 1 | 1 | 1 |
| 1 | 1 | 1 | 1 | 1 | 0 |
| 0 | 1 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 0 | 0 | 0 |
| 1 | 1 | 0 | 1 | 1 | 1 |
| 0 | 1 | 1 | 0 | 1 | 0 |
|  | F3 |  |  | F4 |  |

|  |  |  |
| --- | --- | --- |
| 0 | 1 | 0 |
| 1 | 1 | 1 |
| 0 | 1 | 0 |
|  | K |  |

* Với F2, SUM (F2 ^ K) = 3 thỏa mãn điều kiện nhúng và bít cần nhúng là 0.

Bít dữ liệu nhúng

0 1 0

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | F1’ |  |  | F2' |  |
| 1 | 1 | 0 | 1 | 1 | 1 |
| 1 | 1 | 1 | 1 | 1 | 1 |
| 0 | 1 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 0 | 0 | 0 |
| 1 | 1 | 0 | 0 | 1 | 1 |
| 0 | 1 | 1 | 0 | 1 | 0 |
|  | F3’ |  |  | F4’ |  |

Vì SUM (F2 ^ K) mod 2 = 3 mod 2 # 0 và 1 < SUM (F2 ^ K) < SUM (K) – 1 nên ta chọn ngẫu nhiên một vị trí để đảo bit trong khối F2, chẳng hạn vị trí (2,3) thỏa mãn K [2,3] =1 (theo trường hợp 4). Sau khi đảo bit F2 [2,3] ta thu đƣợc khối F2 , như trên sơ đồ minh họa (bit bị đảo được tô xám).

* Với F3, SUM (F3 ^ K)= 3 thỏa mãn điều kiện nhúng và bit cần nhúng là 1. Ta có SUM (F3 ^ K) mod 2 = 3 mod 2 = 1 = b. Khối F’ thu được giữ nguyên khối F3 nhung với ý nghĩa là khối đã được giấu bit = 1 (theo trường hợp 1)
* Với F4, SUM (F4 ^ K) = 4 thỏa mãn điều kiện nhúng và bit cần nhúng là 1. Ta có SUM (F4 ^ K) mod 2 = 4 mod 2 = 0 # b và SUM (F4 ^ K) = SUM (K) – 1. Theo trường hợp 3 trong thuật toán, ta chọn vị trí (2,1) để đảo bit trong khối F4 vì với phần tử này ta có F4[2,1] = 1 và K [2,1] =1 . Sau khi đảo bit F4 [2,1] ta thu được khối F4’ như trên hình vẽ (bit bị đảo được tô xám).

#### 2.2.6.2. Quá trình tích thủy vân.

phương pháp giấu tin Wu- Lee cho phép giấu nhiều nhất 1 bit dữ liệu trong 1 khối, Giả sử có được bất biến 0 < SUM (Fi ^ K) < SUM (K).

Trong thuật toán nhúng tin, tiến hành đảo 1 bit trong mỗi khối Fi, sao cho tổng số bit 1 của Fi ^ K bằng tổng số bit 1 của K tức là :

SUM (Fi ^ K) = [b mod 2]

Do đó, khi xác định được 0 < SUM (Fi ^ K) < SUM ( K) thì có nghĩa là khối đó có giấu tin, Bit tin được giấu xác định bởi công thức:

b= [SUM (Fi’ ^ K)] mod 2

#### Nhận xét.

Việc chọn khóa K nhằm làm tăng độ bảo mật của thuật toán. Nếu thuật toán 1 chỉ biết kích thước khối là M×N thì đối phƣơng rất dễ khai thác thủy vân.

Phép toán Fi ^ K quy định thuật toán chỉ đƣợc phép sửa các bit trong khối Fi ứng với bit 1 trong khóa K. Như vậy, khóa K được xem như một mặt nạ, tạo ra khung nhìn cho thuật toán. Ta có thể thay phép toán ^ bằng một phép toán khác chẳn hạn phép + .

Điều kiện 0< SUM (Fi ^ K) < SUM (K) quy định nếu khối Fi ^ K toàn 0 hoặc giống như khóa K thì không được giấu tin để tránh bị lộ.

Do việc giấu tin vào khối chỉ cần thay đổi tối đa một bit nên việc chọn bit nào trong F để đảo cần tuân thủ theo nguyên tắc: Nếu Fi ^ K có nhiều bit 1 thì chọn bit 1 , ngược lại nếu Fi ^ K có quá it bit 1 thì chọn bit 0. Nguyên tắc này làm giảm khả năng bit đảo bị phát hiện.

Vì khóa K là bí mật nên thông tin đã nhúng là bí mật. Thuật toán này đã thay đổi nhiều nhất của một bit của khối Fi khi giấu một bit thông tin vào bên trong khối nên với một khối có kích thước M×N đủ lớn thì sự thay đổi của Fi là nhỏ.

Ảnh F được lựa chọn để nhúng tin có quá nhiều điểm trắng hay quá nhiều điểm đen đều làm giảm tỷ lệ bít giấu đƣợc.

Thuật toán Wu – Lee đơn giản, lượng tin giấu được không thấp nhưng tính bảo mật không cao, không thích hợp với ảnh có mảng đen và trắng rộng.

# Chương III : Phương Pháp Nghiên Cứu Cơ Chế Giấu Tin Trong Ảnh và Ứng Dụng Trong Mã hóa Dữ Liệu

3.1. Yêu Cầu bài Toán

* Tính ẩn của giấu tin được chèn vào ảnh: Sự hiện diện của giấu tin trong ảnh không làm ảnh hưởng tới chất lượng của ảnh đã chèn tin.
* Tính bền của giấu tin: Cho phép các tin có thể tồn tại được qua các phép biến đổi ảnh, biến dạng hình học hay các hình thức tấn công cố ý khác.
* Tính an toàn: Chỉ có bên nhận được cấp một khóa và bằng các kỹ thuật tách ảnh phù hợp mới có thể lấy được tin trong ảnh.
  1. Phương Pháp Đề Xuất

Xây dựng phần mềm mã hóa thông tin (sử dụng AES) dấu tin trong ảnh, áp dụng kỹ thuật thủy vân LSB.

### Giới thiệu về kỹ thuật thủy vân LBS(Least Signification Bit)

Về cơ bản, kỹ thuật thủy vân LBS dựa trên tần suất xuất hiện của các bit 0 và 1 trong file ảnh gốc và trong thông điệp cần mã hóa, từ đó đưa ra sự thay thế các bit này để thực hiện việc giấu tin .

Cụ thể hơn, trong kỹ thuật thủy vân LSB, bit cuối cùng của mỗi byte được đặt giá trị 0, sau đó tùy thuộc vào giá trị 0 hoặc 1 của dữ liệu mà thay đổi. Nếu bit của dữ liệu là 0 thì giữ nguyên, còn nếu bit của dữ liệu là 1 thì sẽ đổi giá trị này trên ảnh thành 1.

Để thực hiện kỹ thuật thủy vân này, cần một ảnh gốc, hay còn gọi là cover image. Do phương pháp này sử dụng những bits của từng pixcel trong ảnh, nó đòi hỏi một định dạng nén không mất thông tin. Khi ta sử dụng ảnh màu 24 bit, từng bit của mỗi màu thành phần R, G, B đều có thể đƣợc sử dụng, nhƣ vậy có thể giấu được 3 bit trong mỗi điểm ảnh, đồng nghĩa với việc nhúng đƣợc nhiều thông tin hơn.

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 16 bit thì 15 bit 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 8 bit biểu diễn mỗi điểm ảnh của ảnh 256 màu.

Mỗi điểm ảnh biểu diễn bởi 8 bit bit cuối cùng được coi là bit ít quan trọng nhất tức là bit bên phải nhất.

|  |  |  |
| --- | --- | --- |
| 1001110 0 | 10010101 | 11100010 |

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.

### 3.2.2. Quá trình nhúng thủy vân.

#### 3.2.2.1 InPut:

* Ảnh gốc.
* Dữ liệu thủy vân.
* Khóa bí mật

Khóa bí mật là 1 chuỗi ký tự được tạo nên từ kết quả của bộ hàm  mnemonic bip0032

Ví dụ :

* Chuỗi người dung nhập "00000000000000000000000000000000"
* Chuỗi mnemonic English :

            "abandon abandon abandon abandon abandon abandon abandon abandon abandon abandon abandon about".

* Mầm khóa (PBKDF2 (HMAC-SHA256,4096,256)) :

   "c55257c360c07c72029aebc1b53c05ed0362ada38ead3e3e9efa3708e53495531f09a6987599d18264c1e1c92f2cf141630c7a3c4ab7c81b2f001698e7463b04",

* Khóa bí mật (được tạo ra từ bộ hàm BIP39) :

           "xprv9s21ZrQH143K3h3fDYiay8mocZ3afhfULfb5GX8kCBdno77K4HiA15Tg23wpbeF1pLfs1c5SPmYHrEpTuuRhxMwvKDwqdKiGJS9XFKzUsAF"

#### 3.2.2.2 OutPut:

* Ảnh mang: có chứa thông tin thủy vân. Ảnh mang có sự thay đổi không đáng kể so với ảnh gốc.
* Để có thể lưu trữ lượng thông tin lớn và sự thay đổi màu sắc của ảnh là không đáng kể, chúng ta sử dụng file bitmap 24 bit . Cụ thể hơn, một pixel 26 của ảnh được biểu diễn 3 màu đỏ, xanh lá cây và xanh da trời (R|, G, B), mỗi màu sử dụng 8 bit. Tuy nhiên trong lược đồ trình bày dưới đây, chúng ta chỉ sử dụng bit cuối cùng màu xanh da trời để giấu thông tin.

#### 3.2.2.3 Thực hiện

* Bước 1 : Tính tổng số bytes cần dùng để nhúng thủy vân. Giá trị này được lưu trong biến int S.
* Bước 2 : Đọc các kí tự từ file text sau đó chuyển giá trị ASCII của chúng sang dạng nhị phân 8 bit, lưu giữ trong một mạng từ A [7] về A [0] (A[0] là LSB).
* Bước 3 : Tính toán xem có tất cả bao nhiêu bit 0 và 1 xuất hiện trong mỗi byte, lưu tổng các giá trị này lần lượt là i0 và i1.
* Bước 4 :  Lặp lại từ bước 1 -> 4 cho đến khi kết thức toàn bộ văn bản EOF.
* Bước 5 : Từ ảnh gốc , đọc giá trị RGB của mỗi pixel.
* Bước 6 :  Đọc giá trị bit cuối cùng của mỗi pixels. Với ảnh RGB 24 bit thì ta sẽ đọc bit cuối cùng trong số 8 bit của màu xanh da trời.
* Bước 7 : Kiểm tra xem bit này có giá trị 0 hay l, sau đó tính tổng số lần xuất hiện các bit này trong S pixcels, lưu lần lượt vào hai biến c0 và c1.
* Bước 8: Lặp lại từ bước 5 cho đến bước 7 [8\*S] lần. Đây là số pixel cần đọc để có thể giấu toàn bộ các byte thông điệp.
* Bước 9 : Nếu [ (c0 > c1) và (i0 > i1) ] và [ (c1> c0) và (i1>i0)], đặt giá trị cho flag = 0, ngược lại đạt giá trị flag = 1.
* Bước 10 : Ghi giá trị của flag vào phía bên trái của bit cuối cùng của pixel đầu tiên trong ảnh giấu.
* Bước 11 : Mở ảnh gốc ở chế độ đọc. Tạo một ảnh mang giống ảnh gốc ở chế độ ghi.
* Bước 12 : Đọc Header của file gốc. Ghi thông tin header này lên ảnh mang. Từ ảnh gốc, đọc giá trị RGB của mỗi pixel.
* Bước 13 : Đọc bit stream của dữ liệu. Nếu giá trị của cờ là 0 thì giữ nguyên giá trị bit của dữ liệu, sau đó ghi đè lên bit cuối cùng của màu xanh của pixel, ngược lại, nếu giá trị cờ là 1 thì đảo lại bit dữ liệu rời mới ghi lên pixcel (0 thành 1 hoặc 1 thành 0). Ghi pixel này vào ảnh stego.
* Bước 14 : Nếu toàn bộ các LSB đã được sửa đổi thành công, thì ghi nốt các bit còn lại của các pixel vào ảnh mang. Ngược lại, quay lại bước 13.

### 3.2.3. Quá trình tách thủy vân.

#### 3.2.3.1 InPut:

* Hình ảnh chứa thông điệp.
* Khóa AES.
* Khóa bí mật.

#### 3.2.3.2 OutPut

* Thông điệp đầu ra.

#### 3.2.3.3 Thực hiện:

* Bước 1 : Mở ảnh Stego dưới chế độ đọc.
* Bước 2 : Đọc bit liền kề bit cuối của pixel đầu tiên trong ảnh. Dựa trên giá trị của nó, đặt giá trị flag là 0 hoặc 1.
* Bước 3 :  Đọc từng pixel của ảnh Stego.
* Bước 4 : Nếu flag là 0 thì đọc bit cuối cùng của mỗi pixel và đƣa vào một mảng. Ngược lại nếu flag = 1 thì đảo bit rồi mới chuyển vào mảng.
* Bước 5 : Đọc mỗi 8 pixel theo cách trên, sau đó chuyển nội dung của mỗi 8 phần tử của mạng sang hệ thập phân, dây chính là giá trị ASCII của kí tự.
* Bước 6 : Nếu chưa gặp giá trị EOF thì in kí tự và quay lại bước 3.
  + 1. Ví dụ minh họa.
* Giả sử thông tin cần nhúng là Hi. Trong bảng mã ASCII, H có mã là 72 và i có mã là 105 :
* Chuyển sang hệ nhị phân ta có H = 01001000 và i = 01101001.
* Thông điệp Hi được mã hóa có dạng : 0100100001101001.
* Trong chuỗi trên có 6 bit 1 và 10 bit 0 + cần 16 pixel để lưu giữ 16 bit dữ liệu trên.
* Giả sử có một bảng 16 pixel RGB có giá trị như sau:

|  |
| --- |
| 11001000 01100001 10100001  11001011 11110000 10100001  01001111 01000001 10111101  01001111 11110000 10111001  01000000 01000000 10110000  11001111 01010000 10100001  11001111 11100001 10100000  11000000 11110000 10100001  11001111 10010000 10100000  11001111 11110000 10100001  11001111 11110000 10100001  11000011 11110000 00100000  00001111 11110000 00100000  11001111 11010000 10000001  11001111 10110110 10100001  01001111 01110000 10100001 |

* Dựa theo thuật toán ta có : i0 = 10 i1 = 6 c0 = 5 c1 =11.
* Ở đây ta có i0> i1 nhưng c0 < c1 , do đó cần thực hiện phép đổi bit trên thông điệp thành 101101111001010 và đặt flag có giá trị bằng 1.
* Sau quá trình nhúng thủy vân các điểm ảnh của ảnh Stego sẽ có dạng.

|  |
| --- |
| 11001000 01100001 1010000**1**  11001011 11110000 1010000**0**  01001111 01000001 1011110**1**  01001111 11110000 1011100**1**  01000000 01000000 1011000**0**  11001111 01010000 1010000**1**  11001111 11100001 1010000**1**  11000000 11110000 1010000**1**  11001111 10010000 1010000**1**  11001111 11110000 1010000**0**  11001111 11110000 1010000**0**  11000011 11110000 0010000**1**  00001111 11110000 0010000**0**  11001111 11010000 1000000**1**  11001111 10110110 1010000**1**  01001111 01110000 1010000**0** |

Quá trình tách thủy vân tiến hành ngược lại :

* Flag được đọc và nhận giá trị 1.
* Đọc 16 bits cuối của ảnh Stego ta nhận đƣợc chuỗi 1011011110010110.
* Do flag = 1 , ta cần thực hiện phép đảo bit để nhận được chuỗi nguyên bản 0100100001101001.
  1. Phương Pháp Đánh Giá

### Test vector

Sử dụng vector kiểm tra các thành phần của phần mềm hiện thực trong lúc lập trình

Xem thêm các vector ở phụ lục

### Đánh giá mức giai đoạn sử dụng tỉ lệ và tỉ lệ phần tram

Đánh giá theo giai đoạn sử dụng tỷ lệ và tỷ lệ phần trăm cũng là hình thức phổ biến và tồn tại lâu dàu của đánh giá phần mềm. thông thường sẽ có 5 đến 8 pha và các công việc cụ thể như:

(1) thu thập yêu cầu

(2) phân tích và thiết kế

(3) lập trình

(4) kiểm thử

(5) cài đặt và bảo trì.

### Đánh giá mức hoạt động sử dụng cấu trúc phân tích công việc

Đánh giá dựa trên hoạt động hay nhiệm vụ sử dụng cấu trúc phân tích công việc, khác xa với tính chính xác nhất của phương pháp thủ công. Phương pháp đánh giá này xuất hiện vào những năm 1960 cho các dự án phần mềm lớn và đã được chứng minh là một phương pháp mạnh mẽ và có hiệu quả hỗ trợ các hình thức quản lí dự án. Nhược điểm của đánh giá thủ công dựa trên cấu trúc phân chia công việc là quá cặn kẽ, nó chi phối thời gian đánh giá ban đầu, và khó sửa đổi khi yêu cầu thay đổi hoặc điều chỉnh phạm vi của dự án.

# Chương IV : Hiện Thực và Đánh Giá Kết Quả

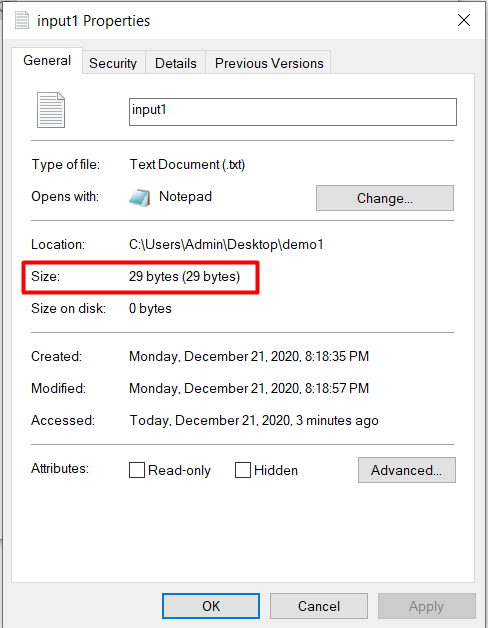
4.1 Tập Dữ Liệu Thử Nghiệm.

### 4.1.1 Tập dữ liệu thử nghiệm 1.

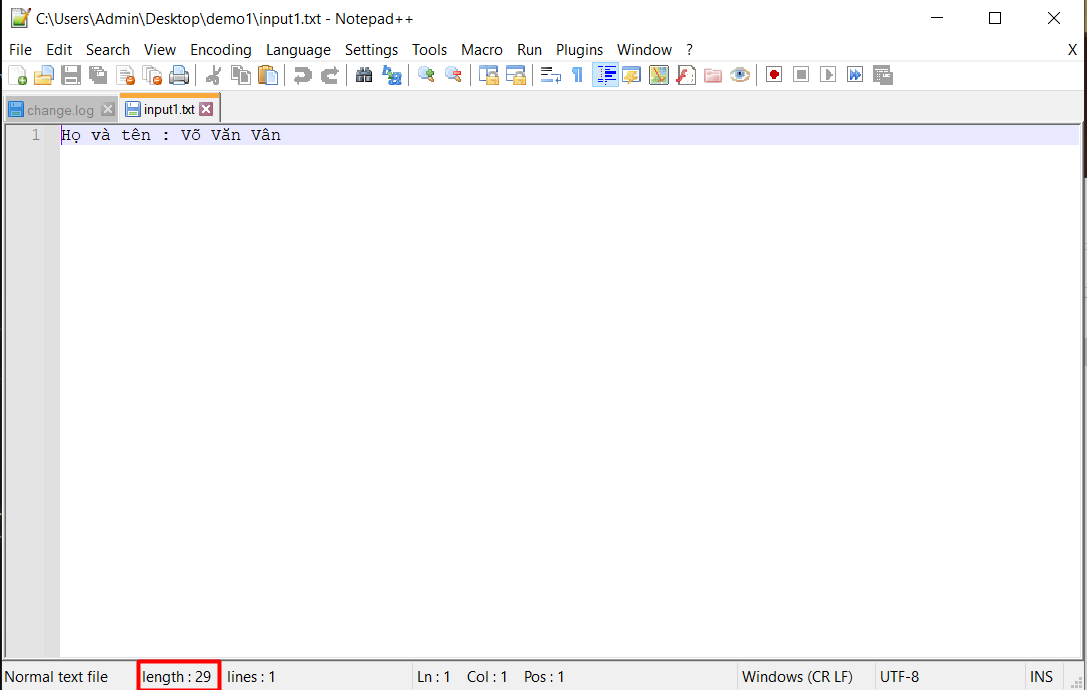
Thông điệp cần chèn:

Nội dung : “Họ và tên : Võ Văn Vân”

Kích thước: 29 Bytes



Số ký tự: 29



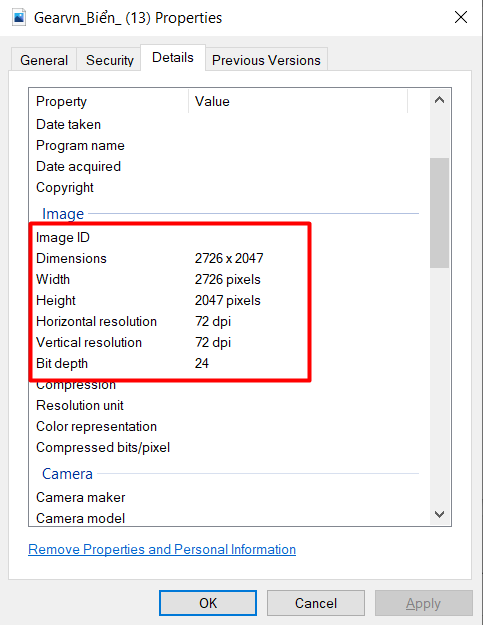
Bảng mã: UTF-8

Hình ảnh đầu vào thử nghiệm 1:

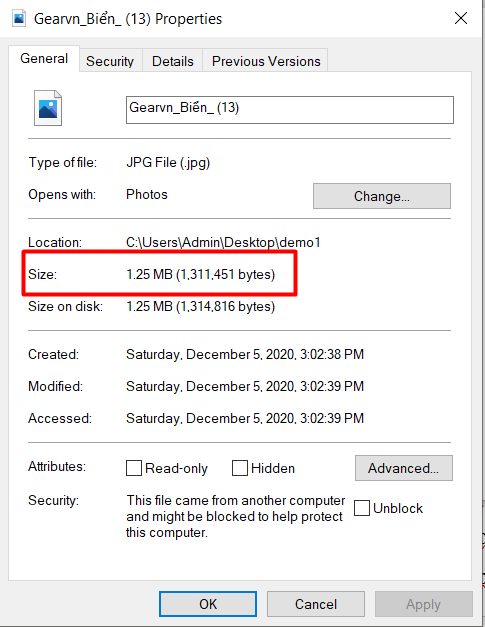
A picture containing outdoor, sky, ground, nature

Description automatically generated

Kích thước : 2726 x 2047 pixel

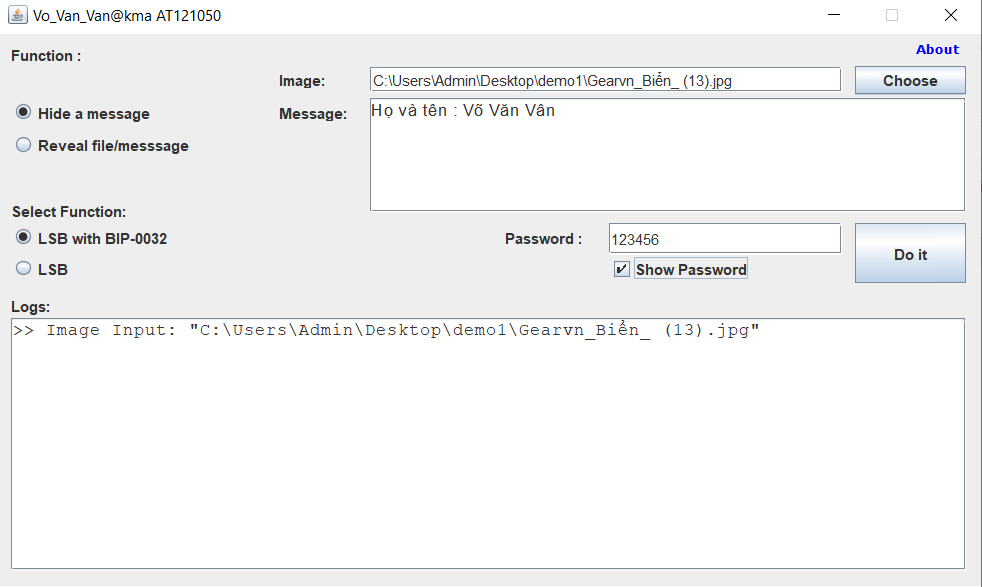


Dung lượng: 1.25 MB



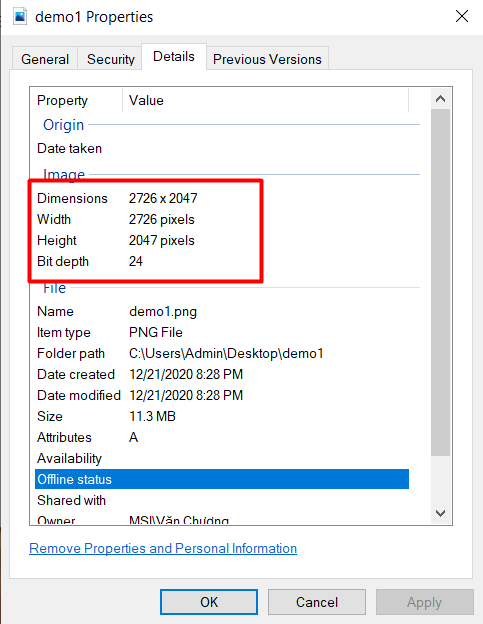
4.2 Thí Nghiệm và Đánh Giá Kết Quả

### 4.2.1 Kết quả của thí nghiệm 1

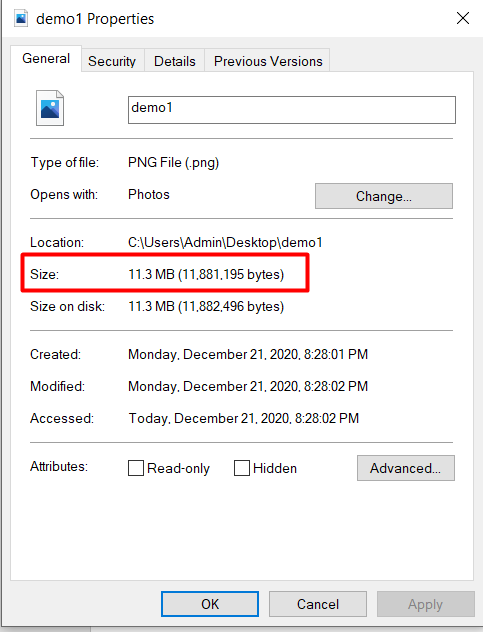


Chú thích hình ảnh:

Kích thước hình ảnh :



Dung lượng



Hình ảnh sau khi nhúng

A picture containing outdoor, sky, ground, nature

Description automatically generated

4.3. Đánh giá kết quả

Dựa vào kết quả của thuật toán và chương trình demo đã thành công ẩn giấu thông tin trong ảnh mà không làm thay đổi hình ảnh.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Tên | | Trước khi nhúng | Sau khi nhúng | Trích xuất |
| Lần 1 | Độ dài text | 29 bytes |  | 29 bytes |
| Kích thước hình ảnh | 2726 x 2047 pixel | 2726 x 2047 pixel | 2726 x 2047 pixel |
| Dung lượng hình ảnh | 1.25M | 11.3M |  |
| File ảnh | JPG | PNG | PNG |
| Lần 2 | Độ dài text | 29 bytes |  | 29 bytes |
| Kích thước hình ảnh | 2726 x 2047 pixel | 2726 x 2047 pixel | 2726 x 2047 pixel |
| Dung lượng hình ảnh | 11.25M | 11.3M |  |
| File ảnh | PNG | PNG | PNG |

# Chương V : Kết Luận

5.1. Kết luận

Qua quá trình nghiên ứu và thực hiện đồ án, đồ án đã hoàn thành tất cả mục tiêu đề ra như sau:

o Hoàn thành tìm hiểu cơ chế giấu tin trong ảnh.

o Hoàn thành tìm hiểu các công trình nghiên cứu liên quan và phân tích ưu nhược điểm của chúng.

o Đề suất được một cơ chế giấu tin trong ảnh.

o Xây dựng thành công một ứng dụng giấu tin trong ảnh.

5.2. Ưu - Nhược Điểm

Phương pháp chèn vào các bit ít quan trọng rất dễ bị tấn công bởi các phép biến đổi, thậm chí là những phép thông thường và ít nguy hại nhất. Các phương pháp nén mất mát thông tin, chẳng hạn như JPEG, gần như là phá vỡ các thông tin bị giấu. Vấn đề là lỗ hỗng của hệ thống tri giác của con người mà phương pháp chèn các bit ít quan trọng cố gắng khai thác – ít nhạy cảm với sự thay đổi nhỏ các giá trị màu của màu xanh hay độ chói -  cũng giống với những gì mà các phương pháp nén mất mát thông tin dựa vào để có thể giảm dung lượng bức ảnh. Các phép biến đổi hình học như di chuyển các điểm ảnh và đặc biệt là đổi chỗ các điểm ảnh so với lưới gốc ban đầu cũng phá hủy các thông tin được nhúng và cách duy nhất để lấy lại thông tin là phải làm các phép chuyển đổi ngược lại. Các phép biến đổi các trên ảnh cũng dễ dàng làm mất các thông tin bị nhúng. Nói tóm lại, phương pháp chèn vào các bit ít quan trọng là phương pháp giấu tin rất ít bền vững.

5.3. Hướng Mở Rộng Tương Lai

Xây dựng lại giao diện ứng dụng cho đẹp hơn

Phát triển ứng dụng thành nhúng được các tệp chương trình thực thi

Nghiên cứu và cải tiến các thuật toán nén, thuật toán nhúng

# Tài Liệu Tham Khảo

* 1. Ingemar J. Cox: Hình mờ kỹ thuật số và steganography. Morgan Kaufmann, Burlington, MA, Hoa Kỳ, 2008
  2. Wayner, Peter (2002). Disappearing cryptography: information hiding: steganography & watermarking. Amsterdam: MK/Morgan Kaufmann Publishers
  3. Wayner, Peter (2009). Disappearing cryptography 3rd Edition: information hiding: steganography & watermarking. Amsterdam: MK/Morgan Kaufmann Publishers
  4. https://github.com/bitcoin/bips/wiki/Comments:BIP-0032

# phụ lục

* 1. Link github toàn bộ đồ án [*https://github.com/kuvanpt2012/StenographyKMA*](https://github.com/kuvanpt2012/StenographyKMA)
  2. Link demo:[*https://github.com/kuvanpt2012/StenographyKMA/tree/main/Demo*](https://github.com/kuvanpt2012/StenographyKMA/tree/main/Demo)
  3. Testvector: *https://github.com/kuvanpt2012/StenographyKMA/tree/main/Test%20vector*