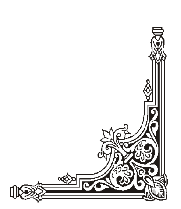
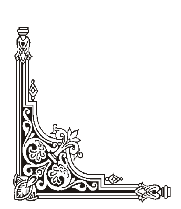
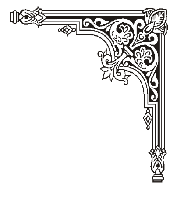
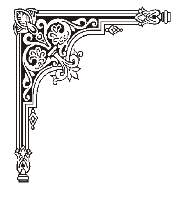
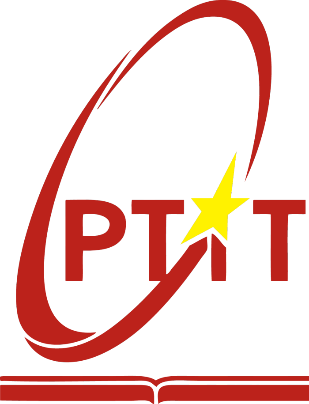
**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**



**KHOA VIỄN THÔNG I**

**----🙣🕮🙡----**

****

**ĐỒ ÁN**

**TỐT NGHIỆP ĐẠI HỌC**

***Đề tài:***

**“Kỹ thuật thủy vân số và ứng dụng trong xác thực ảnh số.”**

|  |  |
| --- | --- |
| **Giảng viên hướng dẫn :** | **TS. PHẠM ANH THƯ** |
| **Sinh viên thực hiện :** | **HOÀNG ĐỨC ANH** |
| **Lớp :** | **D17DCVT009** |
| **Khóa :** | **2017 - 2022** |
| **Hệ :** | **ĐẠI HỌC CHÍNH QUY** |

**HÀ NỘI – 12/2021**

**Lời cảm ơn**

Khi chọn đề tài có tính thực tế cao là “**Kỹ thuật thủy vân số và ứng dụng trong xác thực ảnh số**” làm đồ án tốt nghiệp, chỉ với vốn kiến thức ít ỏi em đã gặp nhiều khó khăn. Nhưng nhờ sự giúp đỡ của cũng như chỉ đạo tận tình của cô Thư em đã khắc phục được thiếu sót trong kiến thức của bản thân, có được kiến thức quý báu để hoàn thành được bài đồ án này

# **CHƯƠNG I: TỔNG QUAN VỀ HỆ THỐNG THỦY VÂN SỐ.**

## **1.1. Khái niệm thủy vân số**

Thủy vân số là quá trình sử dụng các thông tin (ảnh, chuỗi bít, chuỗisố) nhúng một cách tinh vi vào dữ liệu số (ảnh số, audio, video hay text) nhằmxác định thông tin bản quyền của tác phẩm đó. Mục đích của thủy vân số là bảo vệ bản quyền cho phương tiện dữ liệu số mang thông tin thủy vân. Thao tác đưa thủy vân vào một môi trường được gọi là thủy vân số.

Thủy vân số được xem như là một hình thức ẩn giấu tin. Theo sơ đồ phân loạikỹ thuật giấu tin của A.P. Pentitcolas 1999 theo hai hướng nghiên cứu chính là giấu tin mật và thủy vân số. Có thể xem WaterMark là thao tác mà nhúng tin mà trong đó người dùng đầu cuối không cần quan tâm tới thông tin được giấu bên trong đối tượng chứa tin.Thuật ngữ WaterMark cũng bắt nguồn từ cách mà người ta dùng một loại mực vô hình viết lên giấy và chỉ hiển thị lên khi nhúng giấy vào nước.Thuật ngữ thủy vân số cũng được cả cộng đồng thế giới chấp nhận vào những thập niên 1990. Khoảng năm 1995, sự quan tâm đến thủy vân số bắt đầu phát triển nhanh.

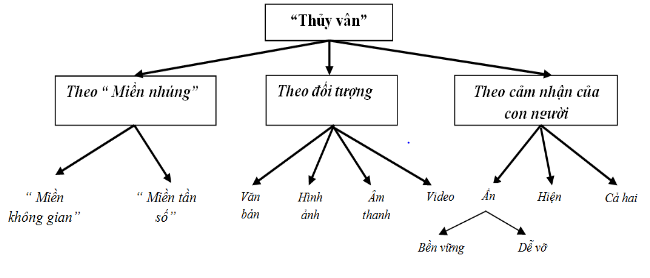
Thủy vân số là quá trình sử dụng các thông tin (ảnh, chuỗi bít, chuỗi số) nhúng một cách tinh vi vào dữ liệu số (ảnh số, audio, video hay text) nhằm xác định thông tin bản quyền của tác phẩm đó. Mục đích của thủy vân số là bảo vệ bản quyền cho phương tiện dữ liệu số mang thông tin thủy vân. Thao tác đưa thủy vân vào một môi trường được gọi là thủy vân số.

Thủy vân số được xem như là một hình thức ẩn giấu tin. Theo sơ đồ phân loại kỹ thuật giấu tin của A.P. Pentitcolas 1999 theo hai hướng nghiên cứu chính là giấu tin mật và thủy vân số. Có thể xem WaterMark là thao tác mà nhúng tin mà trong đó người dùng đầu cuối không cần quan tâm tới thông tin được giấu bên trong đối tượng chứa tin.

Như vậy, thủy vân số là quá trình nhúng dữ liệu vào một đối tượng đa phương tiện theo một phương pháp nào đó, để xác định nguồn gốc của sản phẩm bằng cách trích suât thủy vân.Thủy vân là một phần của dặc trưng của thông tin nhúng trong dữ liệu bảo vệ. Một yêu cầu cảu thủy vân là khó để trích suất hoặc gỡ bỏ được nó từ đối tượng từ khóa thủy vân mà không biết được khóa bí mật.

**1.2. Phân loại thủy vân**

Tùy vào tiêu chí ta có thể chia và phân loại kỹ thuật thủy vân thành nhiều loại khác nhau như sau:



- Phân loại thủy vân theo miền nhúng:

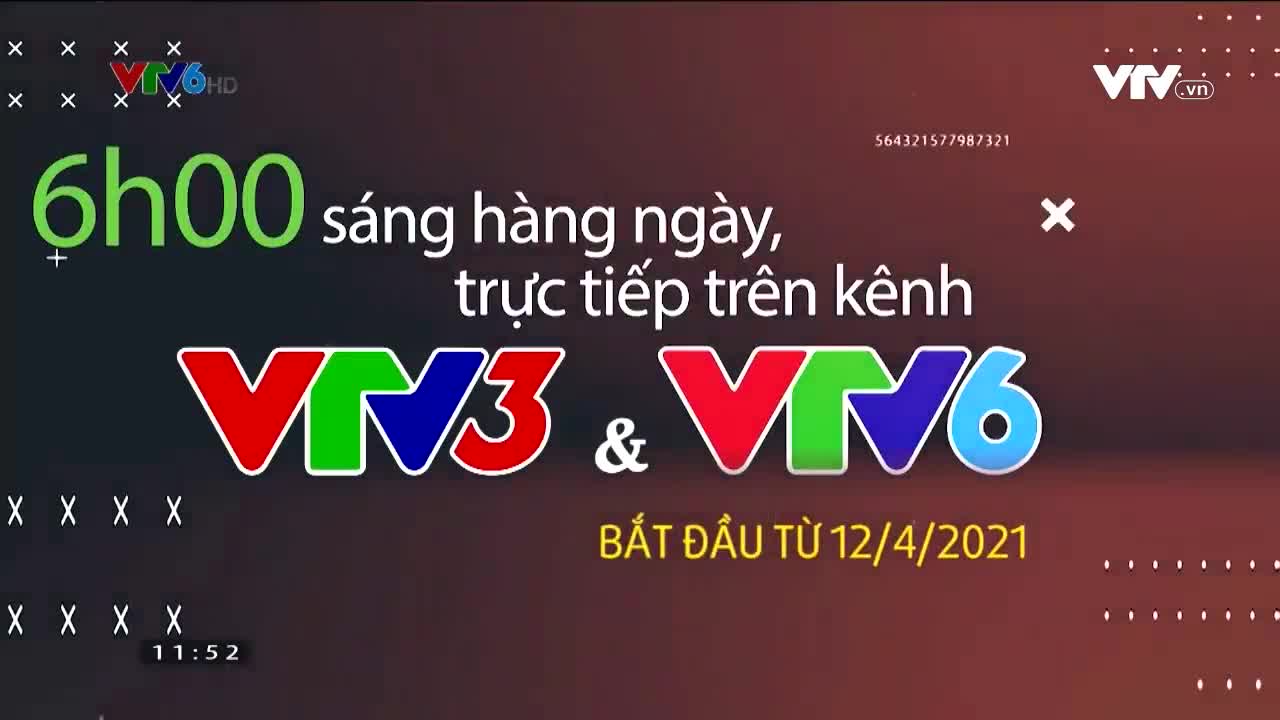
Một trong những tiêu trí để phân lại thủy vân là miền nhúng, miền nhúng là nơi chứ thủy vân. Ví dụ, thủy vân có thể thực hiện trong miền không gian.

- Phân loại thoe đối tượng thủy vân:

Kỹ thuật thủy vân có thể được phân loại theo đối tượng đa phương tiện  
cần nhúng thủy vân như sau:  
+ Thủy vân trên ảnh  
+ Thủy vân trên video  
+ Thủy vân trên âm thanh  
+ Thủy vân trên văn bản  
- Phân loại theo cảm nhận con người:

Tùy theo cảm nhận của con người, thủy vân có thể được chia ba loại  
khác nhau như sau:  
+ Thủy vân hiện: Thuỷ vân hiện là loại thuỷ vân được hiện ngay trên sản phẩm và

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 ti vi mà chúng ta thường thấy như 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 hiện thị ngay trên sản phẩm.



+ Thủy vân ẩn bền vững: được nhúng bằng cách thay đổi trên điểm ảnh sao cho hệ thống cảm giác của con người không thể nhận thấy và phải chịu được các thông tác xử lý tín hiệu thông thường “tấn công” và nó chỉ có thể được phục hồi với cơ chế giải mã thích hợp mà thôi. Xét theo tính bí mật của thủy vân bền vững được phân loại nhỏ hơn như sau :  
+ Lược đồ “thủy vân” bí mật : Cần tới ảnh gốc để trích xuất thủy vân. Có 2 loại lược đồ thủy vân bí mật :

Loại 1: yêu cầu cả ảnh bị biến đổi và ảnh gốc khi trích xuất thủy vân. Ảnh  
gốc được sử dụng để tìm kiếm vị trí thủy vân trong bức ảnh bị biển đối.

Loại 2: trong đó yêu cầu một bản sao của thủy vân trong quá trình trích xuất và kiểm tra mới có thể biết được thủy vân có ở trong bức ảnh cần kiểm tra hay không.

Trong hai loại trên khi trích xuất thủy vân cần đòi hỏi có chìa khóa bí mật.

Đối với loại thứ nhất thì chìa khóa bí mật ở đây là ảnh gốc, còn đối với loại chìa khóa thứ 2 thì chìa khóa bí mật là dữ liệu bí mật được sử dụng để nhúng vào bức ảnh (hay nói cách khác là thủy vân )





Ví dụ về thủy vân ẩn và hiện

- Lược đồ thủy vân nửa bí mật:

Không sử dụng ảnh gốc trong quá trình xác định thủy vân. Tuy nhiên, lược đồ này chỉ đưa ra thông tin có sự hiện diện của thủy vân hay không .

- Lược đồ thủy vân mù:

Trong lược đồ này, không yêu cầu ảnh gốc lẫn thủy vân được nhúng trong quá trình trích thủy vân.

- Lược đồ thủy vân khóa công khai:

Còn được gọi là thủy vân bất đối xứng. Trong lược đồ này, chìa khóa để tìm kiếm và trích xuất thủy vân được công khai với mọi người trái ngược với thủy vân bí mật chìa khóa để tìm kiếm và trích xuất thủy vân là chìa khóa bí mật. Biết đuọc khóa công khai “khó ” mà tính được khóa bí mật và khóa bí mật được sử dụng để nhúng và loại bỏ thủy vân.

+ Thủy vân ẩn dễ vỡ :được nhúng theo cách mà bất kỳ biến đổi hay giả mạo đều làm thay đổi hay phá hủy “thủy vân”.

+ Thủy vân hiện và ẩn đồng thời : (dual watermark) là sự kết hợp giữa thủy vân ẩn và thủy vân hiện  
**1.3. Mô hình thủy vân số**

**1.3.1. Tạo thủy vân số**

Thủy vân có thể là một hình ảnh dạng logo hay văn bản với độ dài cho trước. Thủy vân dạng hình ảnh có khả năng chống chịu trước các phép xử lý ảnh tốt hơn nhiều số với dạng thủy vân dạng ký tự. Thủy vân có thể được biến đổi (bằng mã hóa, chuyển đổi định dạng), trước khi giấu vào ảnh. Các thuật toán nhúng thủy vân dạng logo được gọi là thuật toán thủy vân hợp nhất ảnh. Thủy vân dạng ảnh có lợi ích là dễ dàng nhận biết về mặt trực giác và đưa ra một chứng minh đúng đắn về quyền sở hữu ảnh. Bình thường sẽ có một khóa bí mật K dùng để tăng tính bảo mật cho dữ liệu được nhúng. Do tính bền vững được đảm bảo hơn nên thủy vân dạng ảnh được sử dụng nhiều hơn.

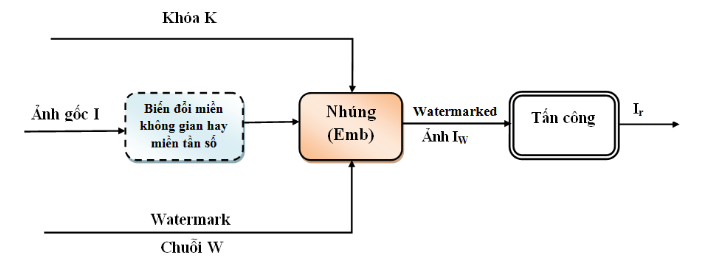
Để tăng thêm tính an toàn và dung lượng thì thủy vân trước khi nhúng vào ảnh mang có thể được mã hóa hay nén lại. Theo cơ chế này, đầu tiên thủy vân số sẽ được nén lại để lượng dữ liệu thủy vân có thể tăng lên, sau đó được mã hóa để tăng tính bảo mật cho thông tin trước khi được giấu vào ảnh mang. Tuynhiên, giải pháp này làm tăng độ phức tạp của bài toán về phát hiện thủy vân.

**1.3.2 Quy trình nhúng thủy vân**

Giai đoạn này gồm thông tin khóa thủy vân, thủy vân, dữ liệu chứa và bộ nhúng thủy vân. Dữ liệu chứa bao gồm các đối tượng như văn bản, audio,video, ảnh…. dạng số, được dùng làm môi trường để giấu tin.

Bộ nhúng thủy vân là chƣơng trình được cài đặt những thuật toán thủy vân và được thực hiện với một khóa bí mật.

Thủy vân sẽ được nhúng vào trong dữ liệu chứa nhờ một bộ nhúng thủy vân. Kết quả quá trình này là được dữ liệu chứa đã nhúng thủy vân được gọi là dữ liệu có bản quyền và phân phối trên các môi trường khác nhau. Trên đường phân phối có nhiễu và sự tấn công từ bên ngoài. Do đó, yêu cầu các kỹ thuật thủy vân số phải bền vững với cả nhiễu và sự tấn công trên.



Hình 1.2 : Quy trình nhúng thủy vân.

Hình 1.2 trình bày và giải thích quá trình nhúng thủy vân cho ảnh tĩnh.

Trong đó, Ảnh gốc được kí hiệu bằng I, “thủy vân” được kí hiệu bởi W, hình ảnh chứa “thủy vân” là Iw và K là khóa nhúng. Hàm nhúng Ew có đầu vào là ảnh gốc I, “thủy vân” W và khóa K và tạo ra một ảnh mới có chứa thủy vân mới thể hiện bằng Iw.

Khóa nhúng K là thực sự cần thiết cho việc nâng cao khả năng bảo mật của hệ thống “thủy vân”. Trước quá trình nhúng, hình ảnh gốc có thể được chuyển đổi sang miền tần số hoặc nhúng có thể được thực hiện biến đổi sang miền không gian. Miền được chọn phụ thuộc vào việc lựa chọn kỹ thuật “thủy vân”. Nếu quá trình nhúng được thực hiện trong miền tần số, biến đổi nghịch đảo được áp dụng để thu được hình ảnh chứa “thủy vân”. Biểu thức toán học cho hàm nhúng có thể được thể hiện như sau:

Đối với kỹ thuật biến đổi theo miền không gian :

**Emb (I, W, K) = Iw**

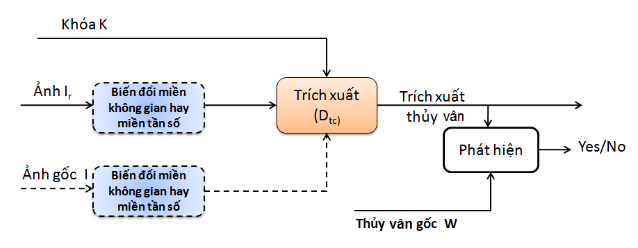
Đối với kỹ thuật biến đổi theo miền tần số :

**Emb (f, W, K) = Iw**

Trong đó f là vecto hệ số cho phép biến đổi.

**1.3.3.Trích xuất và tìm kiếm thủy vân**

Quá trình tách thủy vân được thực hiện thông qua một bộ tách thủy vân tương ứng với bộ nhúng thủy vân cùng với khóa của quá trình nhúng. kết quả thu được là một thủy vân. thủy vân thu được có thể giống với thủy vân ban đầu hoặc sai khác do nhiễu và sự tấn công trên đường đi .



Hình 1.3: Quy trình trích xuất và tìm kiếm thủy vân.

Hình 1.3 trình bày và giải thích quy trình trích xuất và tìm kiếm thủy vân ở trong ảnh tĩnh. Một hàm phát hiện Dtc có đầu vào là hình ảnh Ir có chức năng xác định quyền sở hữu sản phẩm. Các hình ảnh Ir có thể chứa thủy vân hoặc không chứa thủy vân. Trong trường hợp tổng quát, hình ảnh có thể bị biến đổi. Hàm phát hiện có khả năng khôi phục thủy vân We từ bức ảnh hoặc kiểm tra sự hiện diện của thủy vân W trong bức ảnh đã cho Ir hay10 không. Trong quá trình này hình ảnh gốc I cũng có thể yêu cầu, phụ thuộc vào lược đồ thủy vân được lựa chọn. Biểu thức toán học cho thủ tục trích xuất mù (trích xuất không sử dụng ảnh gốc I) cụ thể như sau :

**Dtc (Ir ,K) = W**

Biểu thức toán học cho thủ tục trích xuất không mù (trích xuất có sử dụng ảnh gốc I) cụ thể như sau :

**Dtc (Ir ,I, K) = We**

Thuật toán phát hiện thủy vân mù có đầu ra là một giá trị nhi phân cho biết có sự hiện diện của thủy vân hay không. Bởi vậy, có thể giả sử:

Trong lược đồ tách thủy vân phải được trích xuất một cách chính xác, nguyên mẫu. Lược đồ trích xuất thủy vân có thể chúng mong được quyền sở hữu, trong khi lược đồ phát hiện thủy vân có thể xác nhận có sự hiện diện của thủy vân hay không.  
**1.4. Đặc tính của thủy vân**

Những đặc tính của thủy vân số như:tính bền vững, độ tin cậy phát triển, dung lượng, bảo mật, ... Trong thực tế, không thể thiết kế được một hệ thống đảm bảo tất cả các thuộc tính trên. Ta chỉ có thế đảm bảo cân bằng giữa các thuộc tính.

- Độ trung thực:

Độ trung thực nghĩa là người theo dõi không thể phát hiện ra dấu thủy vân hay nói cách khác dấu thủy vân không làm giảm chất lượng hình ảnh. Đểtín hiệu thực sự là không thể cẩm thấy thì thông tin phải được nhúng vào những bít ít quan trọng. Tuy nhiên, tín hiệu lại dễ dàng bị loại bỏ trong quá trình nên có tổn thất thông tin.

Các nghiên cứu trước đây về thủy vân đều tập trung hầu hết vào việc thiết kế thủy vân không thể thấy được và thường nhúng thủy vân vào trong vùng tín hiệu ít quan trọng về mặt cảm nhận, ví dụ như tần số cao hoặc các bít ít quan trọng. Tuy nhiên, gần đây, các kỹ thuật khác (như kỹ thuật trải phổ)lại chèn giấu thủy ký không thấy được vào trong vùng tín hiệu quan trọng về mặt cảm nhận. Đặt dấu thủy ký trong vùng tín hiệu quan trọng về mặt cảm nhận còn có thể nâng cao tính bền vững chống lại các quá trình xử lý tín hiệu.

- Tính bền vững:

Hình ảnh được thủy vân có thể phải trải qua nhiều loại xử lý biến đổi khác nhau, ví dụ, tăng độ tương phản, lọc thông, làm mờ,…

Do vậy, dấu thủy ký phải có tính bền vững mới chịu được các phép biến đổi ảnh cũng như biến đổi tín hiệu số thành tín hiệu tương tự, tương tự thành số và nén.

Ngoài ra, ảnh chứa thủy vân phải chịu được các phép biến đổi hình học như di chuyển vị trí, co dãn kích thước và cắt xén.

Thủy vân đạt được tính bền vững thực sự khi: dấu thủy vân ký vẫn còn trong dữ liệu sau khi biến đổi và bộ phát hiện/ trích xuất vẫn có thể phát hiện ra thủy vân. Ví dụ, dấu thủy vân vẫn còn tồn tại trong ảnh sau khi phép biến đổi hình học nhưng thuật toán trích xuất/ phát hiện chỉ phát hiện và đưa ra thủy vân sau khi loại bỏ phép biến đổi. Trong trường hợp, không xác định rõ phép biến đổi để thực hiện biến đổi ngược thì bộ phát hiện/ trích xuất không thể phát hiện và đưa ra thủy vân mặc dù thủy vân vẫn tồn tại trong ảnh số.

Thủy vân có thể được nhúng trong hình ảnh bằng cách thay đổi các giá trị điểm ảnh. Trong trường hợp biến đổi miền không gian, thủy vân đơn giản có thể được nhúng vào trong ảnh bằng cách thay đổi các giá trị điểm ảnh hoặc giá trị các bít quan trọng nhất (LSB), CPT . Tuy nhiên, “thủy vân” bền vững hơn nếu được nhúng vào trong miền biến đổi của hình ảnh bằng cách thay đổi các hệ số.

Vào năm 1997, tác giả Cox et.al trình bày một bài báo về “Thủy vân dựa trên trải phổ bảo vệ cho dữ liệu đa phương tiện” và sau đó hầu hết các nổ lực nghiên cứu về các kỹ thuật biến đổi trên miền tần số được dựa trên bài báo này.

-Tính dễ hỏng:

Là thuộc tính đối ngược hoàn toàn với tính bền vững của thủy vân. Thuộc tính này thường được ứng dụng trong lược đồ thủy vân vỡ. Với lược đồ này yêu cầu đặt ra là dấu thủy ký hoặc bị phá hủy bởi bất cứ phương pháp sao chép nào ngoại trừ các phương pháp sao chép hợp pháp. Ví dụ, thủy vân đặt trong một văn bản hợp pháp tồn tại qua bất cứ lần sao chép nào mà không thay đổi nội dung nhưng sẽ bị phá hủy nếu có câu trong nội dung bị thay đổi. Yêu cầu này không giống với chữ ký số trong kỹ thuật mã hóa, trong đó, có thể xác thực tính nguyên vẹn của các bít một cách chính xác nhưng không thể phân biệt các mức biến đổi có thể chấp nhận được.

- Tỉ lệ lỗi sai dương:

Tỉ lệ lỗi sai dương là xác suất hệ thống phát hiện nhầm: xác định một mẩu dữ liệu không mang dấu thủy ký là mang dấu thủy ký. Tùy theo ứng dụng mà ảnh hƣởng của lỗi là khác nhau, trong một số ứng dụng có thể là rất nghiêm trọng. Do đó, trong ứng dụng, người ta phát tính toán trước sao cho tỷ lệ lỗi sai dương nhỏ hơn mức cho phép.

- Tính dư thừa:

Tính dư thừa liên quan đến một thực tế là thủy vân được lặp lại ở những vùng tấn số khac nhau, do đó nếu có một lỗi trên một vùng tần số thì vẫn có thể được khôi phục thông điệp từ các dải tần khác. Tính dư thừa ánh xạ đến tính bền vững, có nghĩa là thủy vân có thể được khôi phục ngay cả khi nó bị biến đổi ở độ nhất dịnh do sự vô ý hay tấn công có chủ ý.

- Đa thủy vân:

Một kẻ tấn công có thể thủy vân lại một đối tượng đã đóng dấu thủy vân và sau đó tuyên bố sản phẩm thuộc quyền sở hữu của mình. Một giải pháp đơn giản nhất trong trường hợp này là gán nhãn thời gian cho thông tin thủy vân với sự có mặt của cơ quan chứng thực hay có thể nhúng thủy vân khác nhau với những người sử dụng khác nhau. Với phương pháp nhúng nhiều thủy vân cho phép lần vết theo nội dung thủy vân nhưng lại tạo điều kiện cho phép tấn công loại bỏ bằng cách lấy trung bình xác suất (tấn công đồng thời).

-Độ phức tạp tính toán

Cũng như bất cứ công nghệ nào sử dụng trong thương mại, độ phức tạp tính toán của lược đồ thủy vân đều rất quan trọng. Điều này, đặc biệt đúng khi sử lý với các dữ liệu thời gian thực.

Mặt khác, cần phải xem xét tính co giãn của độ phức tạp tính toán. Người thiết kế lược đồ thủy vân luôn mong muốn thiết kế được lược đồ mà quy trình nhúng và phát hiện thủy vân có tính co giãn theo các thế hệ của máy tính. Ví dụ, lược đồ thủy vân thế hệ đầu tiên có độ phức tạp tính toán không lớn nhưng độ tin cậy không cao so với lược đồ thủy vân thế hệ tiếp theo. Nhưng khi giải quyết một vấn đề tính toán lớn thì lược đồ thủy vân ở thế hệ sau lại làm việc tốt hơn.

**1.5. Yêu cầu đối với phương pháp thủy vân**

Khi thực hiện thủy vân ảnh số, cần phải có một số tiêu chí để đánh giá chất lượng của giải thuật. Thông thường người ta dựa trên các tính chất sau :

- Bảo đảm tính vô hình

Quá trình thủy vân sẽ làm biến đổi ảnh mang do thủy vân được nhúng vào. Tính “vô hình” thể hiện mức độ biến đổi ảnh mang. Lược đồ thủy vân hiệu quả, sẽ làm cho thủy vân trở nên “vô hình” trên ảnh mang làm cho người khác khó có thể nhận ra, do vậy đảm bảo được tính bí mật của thủy vân. Tuy nhiên trong thực tế không phải khi nào người ta cũng cố gắng để đạt được tính vô hình cao nhất, ví dụ trong thủy vân hiện thủy vân được sử dụng để làm biểu tượng xác thực nguồn gốc sản phẩm, do vậy không nhất thiết phải là bí mật, nhiều khi cần lộ ra cho mọi người biết để mà cảnh giác.

- Khả năng chống giả mạo (tính toàn vẹn):

Đối với thủy vân thì khả năng chống giả mạo là yêu cầu vô cùng quan trọng vì có như vậy mới bảo vệ được bản quyền, minh chứng cho tính pháp lý của sản phẩm. Để có thể chống lại giả mạo thì bất cứ sự thay đổi nào về nội dung của các ảnh số thì thủy vân này sẽ bị hủy đi. Do đó, rất khó làm giả các ảnh số có chứa thủy vân.

- Tính bền vững:

Yêu cầu thứ 3 là thủy vân phải bền vững. Thủy vân phải có khả năng tồn tại cao với các hình thức tấn công có chủ đích và không có chủ đích. Các tấn công không có chủ đích đối với ảnh số bao gồm như nén ảnh, lấy mẫu, lọc, chuyển đối A/D và D/A Tấn công có chủ đích có thể là việc xóa, thay đổi hoặc làm nhiễu thủy vân trong ảnh. Để thực hiện được điều này, thủy ấn phải được dấu trong các vùng quan trọng đối với trực giác. Phương pháp thủy vân phải đám bảo sao cho việc không thể lấy lại thủy vân tƣơng đƣơng với việc ảnh bị biến đổi quá nhiều , không còn giá trị về thương mại .

- Dung lượng:

Với yêu cầu này, thủy vân nhúng vào ảnh phải đủ dùng trong ứng dụng mà không làm thay đổi quá nhiều chất lượng ảnh. Việc giấu thủy vân trong ảnh thì ta bắt buộc phải thay đổi dữ liệu ảnh. ta có thể tăng tính bền vững cho thủy vân bằng cách tăng lượng thay đổi ảnh cho mỗi đơn vị cần giấu. nhưng, nếu thay đổi quá nhiều thì tính ẩn không còn được đảm bảo nữa. Còn nếu thay đổi ảnh quá ít thì các yếu tố dùng để xác định thủy vân trong ảnh sau các phép tấn công có thể không đủ để xác định thủy vân. nếu thông tin được giấu quá nhiều thì cũng dễ làm thay đổi chất lượng ảnh, và làm giảm tính bền vững. Vì vậy, lượng thay đổi ảnh lớn nhất có thể chấp nhận và tính bền vững là nhân tố quyết định cho khối lượng tin được giấu trong ảnh. Trong thực tế, người ta luôn phải cân nhắc giữa chất lượng (tính bí mật, tính toàn vẹn, tính bền vững) và dung lượng thủy vân.

**1.6. Một số ứng dụng của thủy vân**

- Bảo vệ bản quyền ảnh số:

Mặc dù đã có nhiều quy định về bảo vệ bản quyền và đã có những chuyển biến tích cự trong việc thực thi quyền tác giả, nhưng vẫn chưa đủ. Nhưng hành động xâm phạm bản quyền tác giả diễn ra tràn lan, tinh vi và công khai trước sự bất lực của chủ sở hữu. Đặc biệt với dữ liệu số như ảnh số với nhiều định dạng thì vấn đề bảo vệ bản quyền trở nên khó khăn hơn.

Trong việc mua bán và trao đổi các tác phẩm số này nảy sinh các vấn

đề cụ thể như sau:

+ Vấn đề thứ 1 là phải bảo đảm quyền tác giả.: Để bảo vệ được bản quyền của người sở hữu ảnh số thì ảnh số đó phải có những thông tin đặc biệt chứng minh nó là thuộc quyền sở hữu của minh.

+ Vấn đề thứ 2 là đảm bảo thông tin sẵn sang cho người dùng hợp pháp và chống phân phối bất hợp pháp nội dung tác phẩm: mua bán,…

+ Vấn đề thứ 3 lần vết thông tin phát hiện người phân phối sản phậm bất hợp pháp: khi vấn đề về vi phạm bản quyền xảy ra hoặc khi chủ sở hữu sản phẩm số nghi ngờ là có bản sao sản phẩm không hợp lệ.

Đây là ứng dụng cơ bản nhất của kỹ thuật thủy vân. Trong thực tế, nhiều tác phẩm đã có tác quyền nhưng vẫn bị sử dụng sai mục đích. Các thông báo tác quyền này thường được đặt ở một vị trí nào đó trên tác phẩm phân phối.

Do các dấu thủy vân có thể vừa không thể nhìn thấy vừa không thể tách rời tác phẩm chứa nó nên sẽ là giải pháp tốt nhất cho việc bảo vệ bản quyền tác giả. Dấu thủy vân (một thông tin nào đó mang ý nghĩa quyền sở hữu tác giả) sẽ được nhúng vào trong các sản phẩm, dấu thủy vân đó chỉ người chủ sở hữu hợp pháp các sản phẩm đó và được dùng làm minh chứng cho bản quyền sản phẩm.

- Xác thực thông tin và phát hiện xuyên tạc thông tin: dấu thủy vân không chỉ được dùng để chỉ ra thông tin bản quyền tác giả mà còn được dùng để xác thực thông tin và phát hiện ra xuyên tạc thông tin. Dấu thủy vân sẽ được nhúng trong một tác phẩm sau đó được lấy ra và so sánh với dấu thủy vân ban đầu. Nếu có sự sai lệch chứng tỏ tác phẩm gốc đã bị tấn công và xuyên tạc. Các thủy vân nên được ẩn để tránh sự tò mò của đối phương, hơn nữa việc làm giả các thủy vân hợp lệ hay xuyên tạc thông tin nguồn cũng cần xét đến. Trong các ứng dụng thực tế, người ta mong muốn tìm được vị trí bị xuyên tạc cũng như phân biệt được các thay đổi (ví dụ như phân biệt một đối tượng đa phương tiện chứa thông tin giấu bị thay đổi, xuyên tạc nội dung hay chỉ bị nén mất dữ liệu). Yêu cầu chung đối với ứng dụng này la khả năng giấu thông tin cao và thủy vân không bền vững.

- Dấu vân tay hay dán nhãn : thủy vân trong những ứng dụng này được sử dụng để nhận diện người gửi hay người nhận một thông tin nào đó.Ví dụ các vân khác nhau sẽ được nhúng vào các bản copy khác nhau của thông tin gốc trước khi chuyển cho nhiều người.. Những ứng dụng này, yêu cầu là đảm bảo độ an toàn cao cho các thủy vân, tránh khả năng xóa dấu vết trong khi phân phối.

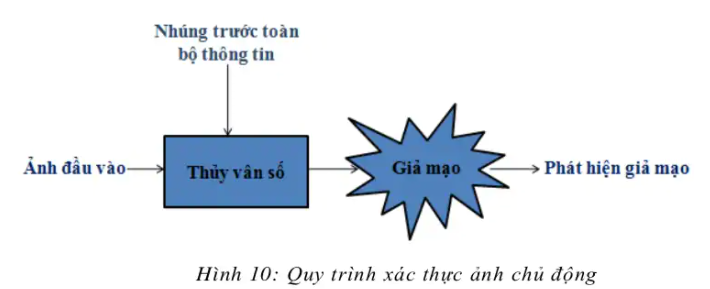
- Điều khiển truy nhập: các thiết bị phát hiện thủy vân (ở đây sử dụng phương pháp phát hiện thủy vân đã giấu mà không cần thông tin gốc) được gắn sẵn vào trong các hệ thống đọc ghi, tùy thuộc vào việc có thủy vân hay không để điều khiển (cho phép/ cấm) truy cập. Ví dụ hệ thống quản lý sao chép DVD được ứng dụng ở nhật.

# **CHƯƠNG II: XÁC THỰC ẢNH SỐ.**

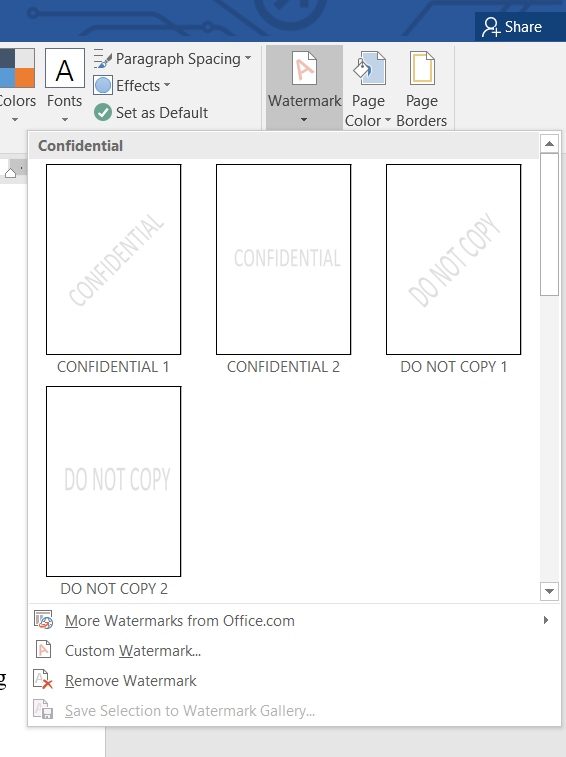
Ta có thể chia các thuật toán và kỹ thuật xác thực ảnh số thành 2 loại chính: Kỹ thuật chủ động và kỹ thuật bị động.

Về cơ bản kỹ thuật xác thực chủ động là nhúng các thông tin cần thiết vào ảnh khi phát hành để bảo về ảnh, tránh bị sao chép.Cũng từ đó ta có thể xác định được nguồn gốc của ảnh.

**2.1 Những kỹ thuật xác thực ảnh chủ động**

****

**-** Thủy vân số: là kỹ thuật nhúng một biểu tượng, chữ ,... vào trong tài liệu số để xác định bản quyền.Kỹ thuật này khá phổ biến ta có thể thấy rất nhiều trong đời sống hằng ngày.Ta cũng có thế xác định bản quyền trong word bằng cách chọn chức năng thủy vẩn ngay trong word (Design/Watermark) ví dụ như sau:



**2.1.1 Kỹ thuật LSB**

Kỹ thuật nhúng thông tin vào bit có trọng số ít nhất là phương pháp đơn giản. Các bit có trọng số thấp nhất có nghĩa là các bit ít quan trọng nhất.Các bit đó đó ít ảnh hưởng tới ảnh. 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 đƣa 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 đƣợc 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.

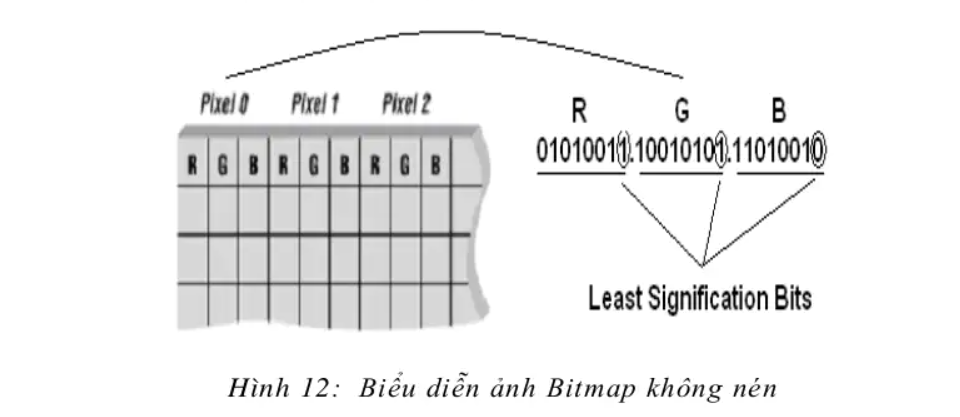
Kỹ thuật LSB ứng dụng cho việc các thực ảnh phải thỏa mãn các tính chất sau:

+ Tính vô hình: Ta sẽ không nhận biết được sự thay đổi bằng mắt thường trước và sau khi nhúng ảnh.

+ Tính không bền vững: Thông tin nhúng trên ảnh phải bị thay đổi khi có sựu tác động dù nhỏ nhất lên ảnh.

+ Tính phân bố:các bit của thông tin nhúng cần đục phân bố đều trên ảnh tránh tập chung một chỗ

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 đƣợc 3 bit trong mỗi điểm ảnh, đồng nghĩa với việc nhúng đƣợc nhiều thông tin hơn.



Trong hình biểu diễn trên mỗi pixel lưu trữ 3 byte ( 3x8=24bit) tương ứng với 3 mầu RBG. Bit khoanh tròn gọi là bit có trọng số thấp nhất ví nếu thay đổi bit đó thì giá trị màu tương ứng cũng chỉ tăng hoặc giảm 1 đơn vị mắt người không thể phân biệt được sự thay đổi đó.Điều này chính là tính vô hình của kỹ thuật thủy vân LSB.

 Dữ liệu vào

+ Ảnh gốc

+ Dữ liệu thủy vân

+ Khóa bí mật

 Dữ liệu ra

+ Ảnh mang: có chứa thông tin thủy vân. Ảnh mang có sự thay đổi

không đáng kể so với ảnh gốc.

+ Để có thể lƣu trữ lƣợng 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 pixel26 của ảnh đƣợc biểu diễn 3 màu đỏ, xanh lá cây và xanh da trời (R|, G, B), mỗi màu sử dụng 8 bit. Tuy nhiên trong lƣợc đồ trình bày dƣới đây, chúng ta chỉ sử dụng bit cuối cùng màu xanh da trời để giấu thông tin.

 Thuật toán nhúng thủy vân:

+ Bƣớc 1 : Tính tổng số bytes cần dùng để nhúng thủy vân. Giá trị này đƣợc lƣu trong biến int S.

+ Bƣớc 2: Đọc các kí tự từ file text sau đó chuyển giá trị ASCII của chúng sang dạng nhị phân 8 bit, lƣu giữ trong một mạng từ A [7] về A [0] (A[0] là LSB)

+ Bƣớc 3: Tính toán xem có tất cả bao nhiêu bit 0 và 1 xuất hiện trong

mỗi byte, lƣu tổng các giá trị này lần lƣợt là i 0 và i1.

+ Bƣớc 4: Lặp lại từ bƣớc 1 -> 4 cho đến khi kết thức toàn bộ văn bản EOF.

+ Bƣớc 5 : Từ ảnh gốc , đọc giá trị RGB của mỗi pixel.

+ Bƣớc 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.

+ Bƣớc 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, lƣu lần lƣợt vào hai biến c 0 và c 1.

+ Bƣớc 8: Lặp lại từ bƣớc 5 cho đến bƣớc 7 [8\*S] lần. Đây là số pixel cần đọc để có thể giấu toàn bộ các byte thông điệp

+ Bƣớc 9: Nếu [ (c0 > c1) và (i0 > i1) ] và [ (c1> c0) và (i1>i0)], đặt gí trị cho flag = 0, ngƣợc lại đạt giá trị flag = 1.

+ Bƣớc 10 : Ghi giá trị của flag vào phía bên trái của bit cuối cùng của

pixel đầu tiên trong ảnh giấu.

+ Bƣớc 11: Mở ảnh gốc ở chế độ đọc. Tạo một ảnh mang giống ảnh gốc ở chế độ ghi.27

+ Bƣớc 12: đọc Header của file gốc. Ghi thông tin header này lên ảnh mang. Từ ảnh gốc, đọc giá trị RGB của mỗi pixel.

+ Bƣớc 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, ngƣợc 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.

+ Bƣớc 14: Nếu toàn bộ các LSB đã đƣợc sửa đổi thành công, thì ghi nốt các bit còn lại của các pixel vào ảnh mang. Ngƣợc lại, quay lại bƣớc 13.

 Thuật toán tách thủy vân

+ Bƣớc 1: Mở ảnh Stego dƣới chế độ đọc

+ Bƣớc 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.

+ Bƣớc 3: Đọc từng pixel của ảnh Stego.

+ Bƣớc 4: Nếu flag là 0 thì đọc bit cuối cùng của mỗi pixel và đƣa vào một mảng. Ngƣợc lại nếu flag = 1 thì đảo bit rồi mới chuyển vào mảng.

+ Bƣớc 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.

+ Bƣớc 6: Nếu chƣa gặp giá trị EOF thì in kí tự và quay lại bƣớc 3.

 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 :

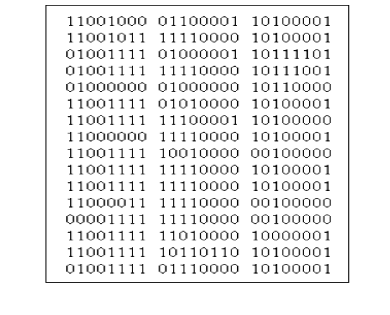
+ Chuyển sang hệ nhị phân ta có H = 01001000 và i = 01101001

+ Thông điệp Hi đƣợc mã hóa có dạng : 0100100001101001

+ Trong chuỗi trên có 6 bit 1 và 10 bit 0

+ cần 16 pixel để lƣu giữ 16 bit dữ liệu trên

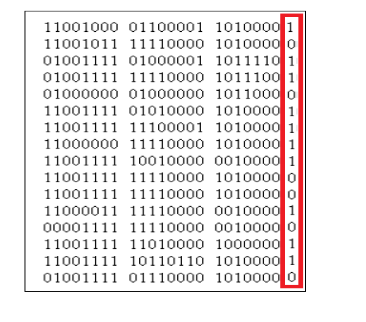
+ Giả sử có một bảng 16 pixel RGB có giá trị



+ Dựa theo thuật toán ta có : i0 = 10 i1 = 6 c0 = 5 c1 =11

+ Ở đây ta có i0> i1 nhƣng 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



Quá trình tách thủy vân tiến hành ngƣợc lại :

+ Flag đƣợc 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 đƣợc chuổi nguyên bản 0100100001101001.

# **CHƯƠNG 3: ỨNG DỤNG THỦY VÂN SỐ TRONG XÁC THỰC ẢNH SỐ.**

Các cuộc tấn công có thể sẩy ra