**TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI**

VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

---------------o0o---------------

**A picture containing food

Description automatically generated**

**MÔN NHẬP MÔN AN TOÀN THÔNG TIN**

**KỸ THUẬT THỦY VÂN SỐ**

**(DIGITAL WATERMARKING)**

**NHÓM 17**

|  |  |
| --- | --- |
| **Họ và tên** | **MSSV** |
| Đỗ Văn Cường | 20172986 |
| Phạm Minh Tiến | 20173397 |
| Mai Đức Trung | 20173417 |
| Nguyễn Sơn Tùng | 20173449 |

**GVHD: PGS. TS. Phạm Linh Giang**

Mục lục

[1. Giới thiệu 3](#_Toc42114844)

[2. Ứng dụng của kỹ thuật thủy vân 3](#_Toc42114845)

[3. Các tính chất của kỹ thuật thủy vân 4](#_Toc42114846)

[3.1 Effectiveness (Hiệu quả) 4](#_Toc42114847)

[3.2 Fidelity (Tính chân thực) 4](#_Toc42114848)

[3.3 Payload size (Kích thước tải trọng) 4](#_Toc42114849)

[3.4 False positive rate (Tỉ lệ dương tính giả) 4](#_Toc42114850)

[3.5 Robustness (Độ bền) 5](#_Toc42114851)

[4. Mô hình thủy vân 5](#_Toc42114852)

[4.1 Mô hình dựa trên góc nhìn truyền thông 5](#_Toc42114853)

[4.2 Mô hình hình học 6](#_Toc42114854)

[5. Kỹ thuật thủy vân không kèm thông tin bên lề 7](#_Toc42114855)

[5.1 Blind embedding và bộ phát hiện sử dụng tương quan tuyến tính 8](#_Toc42114856)

[6. Kỹ thuật thủy vân với thông tin bên lề 12](#_Toc42114857)

[6.1 Informed embedding và bộ phát hiện sử dụng tương quan tuyến tính 13](#_Toc42114858)

[7. Mã Dirty-paper 17](#_Toc42114859)

[7.1 Hệ thống nhúng dựa trên khối với độ bền cố định – bộ phát hiện hệ số tương quan 18](#_Toc42114860)

[8. Kết luận 19](#_Toc42114861)

[Reference 21](#_Toc42114862)

Danh mục hình ảnh

[Hình 1 Mô hình chuẩn của kênh truyền thông với mã hóa dựa trên khóa 5](#_Toc42114863)

[Hình 2 Miền chân thực chấp nhận được (được xác định bởi MSE) và miền phát hiện (được xác định bởi tương quan tuyến tính) 7](#_Toc42114864)

[Hình 3 Mô hình chuẩn cho kỹ thuật thủy vân không kèm thông tin bên lề 8](file:///C:\Users\MSI\Desktop\HUST\20192\Nhập%20môn%20an%20toàn%20thông%20tin\Bài%20tập%20lớn\Báo%20cáo.docx#_Toc42114865)

[Hình 4 Ví dụ cho kết quả cho hệ thống blind embedding 9](file:///C:\Users\MSI\Desktop\HUST\20192\Nhập%20môn%20an%20toàn%20thông%20tin\Bài%20tập%20lớn\Báo%20cáo.docx#_Toc42114866)

[Hình 5 Giá trị phát hiện hình ảnh nhúng thủy vân 10](file:///C:\Users\MSI\Desktop\HUST\20192\Nhập%20môn%20an%20toàn%20thông%20tin\Bài%20tập%20lớn\Báo%20cáo.docx#_Toc42114867)

[Hình 6 Giá trị phát hiện hình ảnh nhúng thủy vân sau khi áp dụng bộ lọc thông thấp cho mẫu tương quan 11](file:///C:\Users\MSI\Desktop\HUST\20192\Nhập%20môn%20an%20toàn%20thông%20tin\Bài%20tập%20lớn\Báo%20cáo.docx#_Toc42114868)

[Hình 7 Giá trị phát hiện cho hình ảnh nhúng thủy vân với α = 2 11](file:///C:\Users\MSI\Desktop\HUST\20192\Nhập%20môn%20an%20toàn%20thông%20tin\Bài%20tập%20lớn\Báo%20cáo.docx#_Toc42114869)

[Hình 8 Giá trị phát hiện hình ảnh nhúng thủy vân sau khi thêm nhiễu 12](file:///C:\Users\MSI\Desktop\HUST\20192\Nhập%20môn%20an%20toàn%20thông%20tin\Bài%20tập%20lớn\Báo%20cáo.docx#_Toc42114870)

[Hình 9 Dạng chuẩn của các mô hình thủy vân với thông tin bên lề 13](#_Toc42114871)

[Hình 10 Ví dụ về hình ảnh sau khi nhúng thủy vân 15](#_Toc42114872)

[Hình 11 Giá trị phát hiện cho ảnh sử dụng kỹ thuật thủy vân 16](file:///C:\Users\MSI\Desktop\HUST\20192\Nhập%20môn%20an%20toàn%20thông%20tin\Bài%20tập%20lớn\Báo%20cáo.docx#_Toc42114873)

[Hình 12 Giá trị phát hiện cho ảnh sử dụng kỹ thuật thủy vân khi thêm nhiễu 17](#_Toc42114874)

[Hình 13 Viết ký hiệu A trên dirty paper bằng blind và informed writing 18](#_Toc42114875)

# 1. Giới thiệu

Kỹ thuật thủy vân số là hành động ẩn một thông điệp liên quan đến tín hiệu kỹ thuật số (tức là hoạt hình, bài hát, video) vào trong chính tín hiệu đó. Tương tự kỹ thuật giấu tin mật (Steganography), cả hai đều ẩn một thông điệp bên trong một tín hiệu kỹ thuật số. Kỹ thuật này cố gắng che giấu một thông điệp liên quan đến nội dung thực tế của tín hiệu kỹ thuật số, trong khi giấu tin mật, tín hiệu kỹ thuật số không liên quan đến thông điệp và nó chỉ được sử dụng như một vỏ bọc để che giấu sự tồn tại của thông điệp.

Kỹ thuật thủy vân số đã xuất hiện trong nhiều thế kỷ, ban đầu được tìm thấy dưới dạng các thủy ấn trong giấy in và sau đó là các hóa đơn giấy. Tuy nhiên, lĩnh vực thủy vân số chỉ được phát triển trong 15 năm qua và hiện nó đang được sử dụng cho nhiều ứng dụng khác nhau.

Trong các phần sau sẽ trình bày một số ứng dụng quan trọng nhất của kỹ thuật thủy vân số, giải thích một số tính chất quan trọng trong hệ thống thủy vân và đưa ra một cái nhìn tổng quan về những mô hình thủy vân phổ biến được trình bày trong cuốn sách của Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Friedrich và Ton Kalker [1]. Những mô hình cơ bản này sẽ được minh họa thêm bằng cách sử dụng các ví dụ được viết bằng Matlab.

# 2. Ứng dụng của kỹ thuật thủy vân

Sự gia tăng nhanh chóng của các nghiên cứu về kỹ thuật thủy vân hàng thập kỷ qua có bước chuyển biến lớn nhờ những ứng dụng quan trọng của chúng trong quản lý và bảo vệ bản quyền số.

Ứng dụng đầu tiên của kỹ thuật thủy vân chính là giám sát quảng cáo. Điều quan trọng nhất chính là chúng ta có thể theo dõi khi một video cụ thể được phát trên đài truyền hình. Việc đó rất quan trọng với các doanh nghiệp quảng cáo muốn đảm bảo các quảng cáo của họ được phát đúng thời gian đã chi trả. Kỹ thuật thủy vân có thể được sử dụng cho mục đích này. Thông tin dùng để định danh từng video riêng biệt được nhúng trong chính nó nhờ kỹ thuật thủy vân, giúp việc giám sát quảng cáo dễ hơn.

Một ứng dụng quan trọng khác đó là xác định bản quyền. Khả năng xác định chủ sở hữu của một tác phẩm nghệ thuật số, ví dụ như là một video hay hình ảnh có thể rất khó. Tuy vậy việc đó lại rất quan trọng, đặc biệt trong các vụ việc liên quan tới vi phạm bản quyền. Do đó, thay vì để các lưu ý về bản quyền, ta có thể sử dụng kỹ thuật thủy vân để nhúng bản quyền vào từng hình ảnh hay bài hát.

Truy vết giao dịch là một ứng dụng thú vị khác của kỹ thuật thủy vân. Trong trường hợp này, thủy vân được nhúng trong một sản phẩm kỹ thuật số có thể sử dụng để ghi lại các giao dịch diễn ra trong quá khứ của bản sao chép từ sản phẩm này. Ví dụ, kỹ thuật thủy vân có thể sử dụng để ghi lại người nhận của tất cả bản sao hợp pháp từ một bộ phim, bằng cách nhúng các thủy vân khác nhau với mỗi bản sao. Nếu một bộ phim sau đó bị rò rỉ trên Internet, nhà sản xuất có thể xác định đâu là nguồn gốc cho sự rò rỉ.

Cuối cùng, kiểm soát sao chép là một ứng dụng đầy hứa hẹn của kỹ thuật thủy vân. Nó có thể được sử dụng để ngăn ngừa sao chép trái phép các bài hát, hình ảnh trong phim, bằng cách nhúng trong chúng các thủy vân dùng để chỉ thị các bộ ghi DVD hay CD tương thích kỹ thuật thủy vân không ghi lại bài hát hay bộ phim, vì đó là bản sao bất hợp pháp.

# 3. Các tính chất của kỹ thuật thủy vân

Mỗi hệ thống thủy vân có một số tính chất quan trọng. Các tính chất này thường xung đột với nhau và ta thường buộc phải chấp nhận một vài sự đánh đổi giữa chúng tùy thuộc vào mục đích ứng dụng. Một số tính chất quan trọng bao gồm:

## 3.1 Effectiveness (Hiệu quả)

Đây là tính chất đầu tiên và có lẽ cũng là tính chất quan trọng nhất. Nó thể hiện xác suất mà thông điệp trong hình ảnh nhúng thủy vân sẽ được phát hiện chính xác. Theo một cách lý tưởng thì ta mong muốn xác suất này bằng 1.

## 3.2 Fidelity (Tính chân thực)

Thủy vân là quá trình thay đổi một hình ảnh gốc để thêm vào nó một thông điệp, do đó chắc chắn nó sẽ làm giảm chất lượng hình ảnh. Ta thường muốn để sự suy giảm này ở mức tối thiểu, sao cho không thể nhận ra sự khác biệt rõ rệt nào trong hình ảnh.

## 3.3 Payload size (Kích thước tải trọng)

Mỗi sản phẩm nhúng thủy vân thường mang một thông điệp. Kích thước của thông điệp này thường rất quan trọng vì trong khi có các ứng dụng chỉ cần một bit được nhúng, nhiều hệ thống yêu cầu tải trọng tương đối lớn để nhúng được thông điệp.

## 3.4 False positive rate (Tỉ lệ dương tính giả)

Đây là số sản phẩm kỹ thuật số được xác định có thủy ấn được nhúng trong khi

thực tế chúng không được nhúng một cái nào. Tỉ lệ này nên được giữ ở mức rất thấp cho các hệ thống thủy vân.

## 3.5 Robustness (Độ bền)

Có nhiều trường hợp mà một sản phẩm nhúng thủy vân bị thay đổi trong vòng đời của nó: Do mất mát trên đường truyền hoặc một số cuộc tấn công độc hại nhằm cố gắng loại bỏ thủy ấn hay làm cho nó không thể được phát hiện bởi bên nhận. Một hệ thống thủy vân bền vững có thể chịu được nhiễu Gauss, nén, in, quét, xoay, thu nhỏ, cắt xén và nhiều tác động khác.

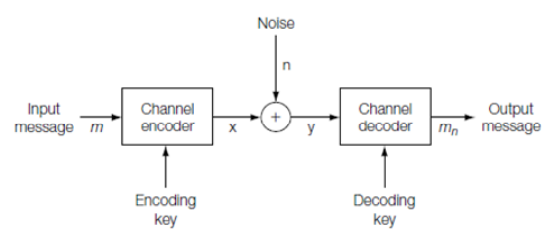
# 4. Mô hình thủy vân

Có một số cách để mô hình hóa một quy trình thủy vân, có thể chia chúng thành 2 nhóm. Nhóm đầu tiên chứa các mô hình dựa trên góc nhìn truyền thông và nhóm thứ hai chứa các mô hình dựa trên góc nhìn hình học.

## 4.1 Mô hình dựa trên góc nhìn truyền thông

Các mô hình này mô tả hệ thống thủy vân theo cách rất giống với các mô hình truyền thông truyền thống. Thủy vân trên thực tế là một quá trình truyền thông điệp từ bên nhúng thủy vân đến bên nhận. Do đó, rất thích hợp khi sử dụng các mô hình truyền thông an toàn để mô hình hóa quá trình này.

Trong một mô hình truyền thông bảo mật phổ biến, có người gửi ở một bên, sẽ mã hóa thông điệp bằng một loại khóa mã hóa nào đó để ngăn kẻ nghe trộm giải mã thông điệp nếu thông điệp bị chặn trong khi truyền. Sau đó, thông điệp sẽ được truyền đi trên một kênh truyền, điều này có thể gây nhiễu cho thông điệp được mã hóa. Thông điệp sẽ được nhận ở đầu kia trên kênh truyền của người nhận, họ sẽ cố gắng giải mã nó bằng khóa giải mã, để lấy lại thông điệp gốc. Quá trình này có thể được nhìn thấy trong Hình 1.



Hình Mô hình chuẩn của kênh truyền thông với mã hóa dựa trên khóa

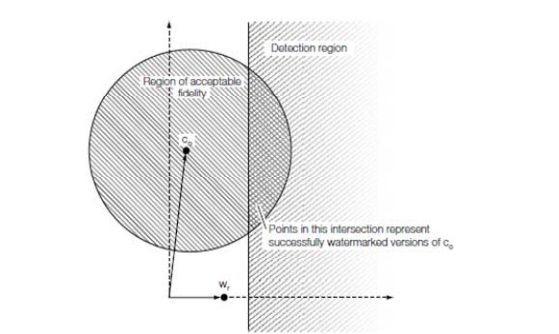
Nói chung, các mô hình thủy vân dựa trên truyền thông có thể được chia thành hai loại phụ. Loại thứ nhất sử dụng thông tin bên lề để tăng cường quá trình thủy vân và loại thứ hai hoàn toàn không sử dụng thông tin bên lề. Thuật ngữ “thông tin bên lề” đề cập đến bất kỳ thông tin phụ trợ nào ngoại trừ chính thông điệp đầu vào, có thể được sử dụng để mã hóa hoặc giải mã nó tốt hơn. Ví dụ tốt nhất về điều này là hình ảnh mang thông điệp, dùng để cung cấp thông tin hữu ích giúp tăng cường phát hiện chính xác thông điệp tại bên nhận.

## 4.2 Mô hình hình học

Tiếp cận kỹ thuật thủy vân theo hướng hình học thường rất hữu ích. Trong loại mô hình này, hình ảnh nhúng thủy vân hay chưa nhúng thủy vân, có thể được xem như các vectơ nhiều chiều trong không gian “media”. Đây là một không gian đa chiều chứa tất cả các hình ảnh có thể có với mọi kích thước. Ví dụ, hình ảnh 512 X 512 sẽ được mô tả dưới dạng vector 262144 phần tử trong không gian 262144 chiều.

Các mô hình hình học có thể rất hữu ích để hình dung rõ hơn quá trình thủy vân bằng cách sử dụng một số miền dựa trên các đặc tính của thủy vân. Một trong những miền này là **miền nhúng** - miền chứa tất cả các hình ảnh có thể có nhờ việc nhúng một thông điệp bên trong một hình ảnh. Một miền quan trọng khác là **miền phát hiện**, đó là miền bao gồm tất cả hình ảnh mà từ đó có thể trích xuất thủy vân thành công. Cuối cùng, **miền chân thực chấp nhận được** chứa tất cả các hình ảnh được nhúng thủy vân mà về cơ bản trông giống hệt với hình ảnh gốc. **Miền nhúng** phải nằm trong miền giao nhau của **miền phát hiện** và **miền chân thực chấp nhận được**, để tạo ra các thủy vân có thể được phát hiện thành công mà không làm thay đổi nhiều đến chất lượng hình ảnh.

Một ví dụ về mô hình hình học có thể được nhìn thấy trong Hình 2. Ở đây ta có thể thấy rằng nếu sai số bình phương trung bình (MSE) được sử dụng như một thước đo độ chân thực, thì miền chân thực chấp nhận được sẽ là một khối cầu n chiều có tâm là hình gốc (co), với bán kính được xác định bởi sai số MSE lớn nhất chấp nhận được. Miền phát hiện cho “thuật toán phát hiện dựa trên tương quan tuyến tính” được xác định bằng một nửa không gian, dựa vào ngưỡng được sử dụng để quyết định hình ảnh có nhúng thủy vân hay không. Lưu ý rằng sơ đồ chỉ là hình chiếu của không gian n chiều vào không gian 2d



Hình Miền chân thực chấp nhận được (được xác định bởi MSE) và miền phát hiện (được xác định bởi tương quan tuyến tính)

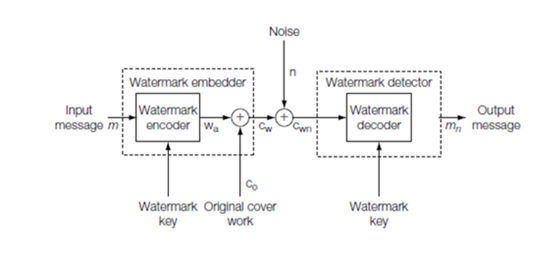
Khi xem xét về các hệ thống thủy vân phức tạp, việc thực hiện một phép chiếu không gian “media” vào một không gian ít chiều có thể sẽ hữu ích hơn. Phép chiếu này có thể được xử lý dễ dàng bởi các máy tính do số lượng phần tử vectơ nhỏ hơn và có thể được biểu thị bằng thuật toán thủy vân dựa trên khối - tách hình ảnh thành các khối thay vì hoạt động trên cơ sở pixel.

# 5. Kỹ thuật thủy vân không kèm thông tin bên lề

Như đã đề cập trước đó, một vài mô hình kỹ thuật thủy vân dựa trên truyền thông không tận dụng được kênh thông tin bên lề. Trong loại mô hình này, hình ảnh đơn giản được coi là một dạng nhiễu làm méo thông điệp trong suốt quá trình truyền tin (hình 3). Bộ nhúng thủy vân mã hóa một thông điệp bằng một mã thủy vân và một khóa. Sau đó được đưa vào hình ảnh gốc rồi truyền qua kênh truyền thông đã được thêm nhiễu. Bộ dò thủy vân ở đầu kia nhận hình ảnh thủy vân bị nhiễu và cố gắng giải mã hình ảnh gốc bằng khóa.

## 5.1 Blind embedding và bộ phát hiện sử dụng tương quan tuyến tính

Hệ thống này là một ví dụ của blind embedding, đó là nhúng thông điệp vào trong hình ảnh nhưng không khai thác những thông số của ảnh gốc. Việc phát hiện được thực hiện bằng cách sử dụng tương quan tuyến tính. Đây là hệ thống kỹ thuật thủy vân 1-bit, nói cách khác, nó chỉ nhúng một bit (bit 1 hoặc 0) vào bên trong ảnh chứa.



Hình 3 Mô hình chuẩn cho kỹ thuật thủy vân không kèm thông tin bên lề

Thuật toán cho bộ nhúng và bộ dò như sau:

**Bộ nhúng:**

1. Chọn ngẫu nhiên 1 mẫu tương quan. Đây đơn giản là một mảng với số chiều bằng với ảnh gốc, có các phần tử được lấy ngẫu nhiên theo phân phối Gauss trong khoảng [-1, 1]. Khóa thủy vân chính là “hạt giống” được dùng cho việc khởi tạo trình sinh số giả ngẫu nhiên, để tạo ra mẫu tương quan ngẫu nhiên.

2. Tính toán một mẫu thông điệp tùy thuộc vào việc nhúng bit 0 hay 1. Nếu là bit 1, giữ nguyên mẫu tương quan ngẫu nhiên. Còn nếu là bit 0, lấy giá trị âm của mẫu tương quan để thu được mẫu thông điệp.

3. Nhân mẫu thông điệp với hằng số α để kiểm soát cường độ nhúng. Giá trị α càng lớn thì độ bền càng lớn, đổi lại, chất lượng hình ảnh giảm. Giá trị α thường khởi tạo = 1.

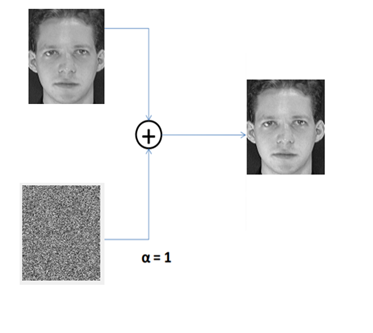
4. Thêm mẫu thông điệp sau khi nhân vào hình ảnh gốc để nhận được hình ảnh nhúng thủy vân.

**Bộ dò:**

1. Tính toán tương quan tuyến tính giữa hình ảnh nhúng thủy vân nhận được và mẫu tương quan ban đầu có thể tạo lại nhờ “hạt giống” khởi tạo được dùng như khóa thủy vân.

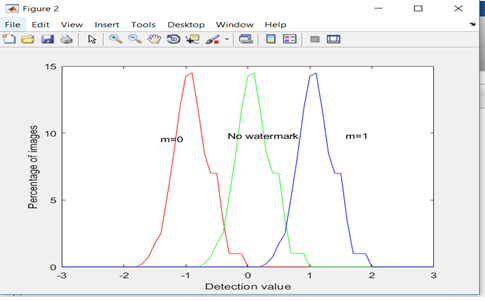
2. Quyết định thông điệp thủy vân là gì dựa trên kết quả của sự tương quan. Nếu giá trị tương quan tuyến tính vượt qua ngưỡng, ta sẽ coi thông điệp là 1. Nếu tương quan tuyến tính nhỏ hơn phần âm của ngưỡng ta sẽ coi thông điệp là 0. Nếu tương quan tuyến tính nằm giữa phần âm và phần dương của ngưỡng, coi như không có thông điệp được nhúng.

Một ví dụ của quy trình nhúng có thể thấy trong hình 4. Hình phía trên bên trái là bức hình gốc, bên dưới là mẫu tương quan và bên phải là hình nhúng thủy vân từ bit 1 với α = 1. Có thể thấy, không có sự khác nhau giữa ảnh gốc và ảnh nhúng thủy vân.



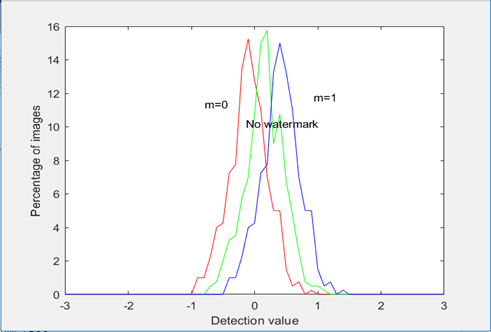
Hình 4 Ví dụ cho kết quả cho hệ thống blind embedding

Để thử nghiệm tính hiệu quả của hệ thống, ta sử dụng 400 hình ảnh kích thước nhỏ (112 X 92 pixels). Ta chạy thuật toán nhúng với α = 1, thử nhúng cả bit 1 và bit 0 với mỗi ảnh, kết quả thu được 800 hình ảnh nhúng. Sau đó tính toán tương quan tuyến tính (như trong bộ dò) cho từng hình ảnh nhúng và hình ảnh gốc rồi phác họa kết quả. Ta có thể thấy trong hình 5. Trục hoành là giá trị của tương quan tuyến tính, còn trục tung là tỷ lệ hình ảnh ứng với giá trị tương quan tuyến tính cụ thể. Có thể thấy, hầu hết hình ảnh nhúng bit 0 có giá trị trung tâm là -1. Những hình nhúng bit 1 có giá trị trung tâm là 1, trong khi đó những hình ảnh không nhúng thủy vân có giá trị trung tâm là 0. Vấn đề là phần giao nhau của 3 đồ thị trong khoảng -1 đến 0 cũng như từ 0 đến 1. Điều đó nghĩa là khó có thể chọn được một giá trị ngưỡng cụ thể vì dù chọn ngưỡng nào, sẽ luôn có những hình ảnh không nhúng thủy vân đuợc phân loại có thủy vân (dương tính giả), trong khi vài hình ảnh khác có nhúng thủy vân lại bị phân loại chưa nhúng thủy vân (âm tính giả). Trong trường hợp lý tưởng, 3 phần đồ thị sẽ không còn giao và cách xa nhau từ đó ta có thể chọn ngưỡng phù hợp.



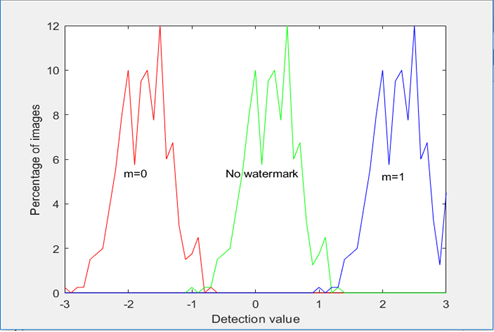
Hình 5 Giá trị phát hiện hình ảnh nhúng thủy vân

Mẫu tương quan cũng rất quan trọng trong hệ thống nhúng thủy vân, đặc biệt là loại hệ thống không chứa thông tin bên lề trong ảnh gốc. Để chứng minh điều này, ta chạy thử nghiệm tương tự như trên, chỉ khác lần này sẽ áp dụng một bộ lọc trung bình thông thấp 2 X 2 trên mẫu tương quan trước khi thêm nó vào từng ảnh. Kết quả thu được trên hình 6. Trục hoành là giá trị tương quan tuyến tính, trong khi trục tung là tỷ lệ hình ảnh ứng với giá trị tương quan tuyến tính cụ thể. Có thể thấy, phần giao nhau của 3 đồ thị rõ ràng hơn nhiều so với thử nghiệm ban đầu. Vì vậy, không thể chọn một ngưỡng thích hợp để có tỷ lệ dương tính giả thấp.



Hình 6 Giá trị phát hiện hình ảnh nhúng thủy vân sau khi áp dụng bộ lọc thông thấp cho mẫu tương quan

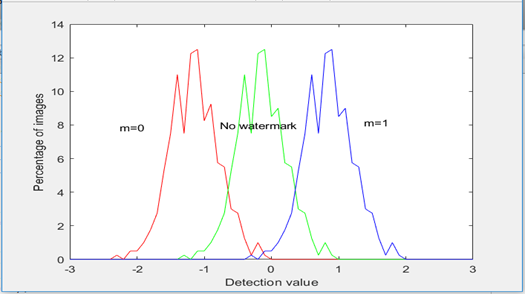
Giá trị α cũng quan trọng không kém, bởi vì nó có thể gia tặng cường độ nhúng bằng cách tịnh tiến các giá trị tương quan tuyến tính ra xa nhau, làm giảm phần giao của 3 đồ thị, ứng với 3 nhóm hình ảnh. Để chứng minh điều này, ta chạy thử nghiệm 400 hình ảnh gốc với α = 2. Kết quả thu được ấn tượng hơn nhiều (Hình 7).



Hình 7 Giá trị phát hiện cho hình ảnh nhúng thủy vân với α = 2

Đồ thị tương quan tuyến tính cho hình ảnh nhúng bit 0 tịnh tiến đến -2 trong khi đồ thị cho hình ảnh nhúng bit 1 tịnh tiến đến 2. Đồ thị cho hình ảnh không nhúng thủy vân nằm trong khoảng 0 và 1. Như vậy đã có sự phân chia rõ ràng giữa 3 đồ thị. Điều đó có nghĩa là ta có thể chọn một ngưỡng phân loại giữa hình ảnh nhúng thủy vân và chưa nhúng thủy vân.

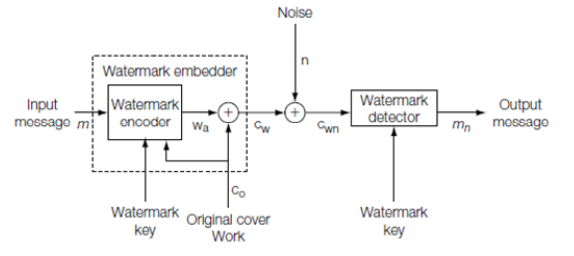
Để thử nghiệm tính bền bỉ của hệ thống, ta chạy một phiên bản sửa đổi của 400 hình ảnh thử nghiệm ban đầu, ta sẽ thêm nhiễu ngẫu nhiên tuân theo phân phối Gauss trong khoảng [-10,10] cho từng điểm ảnh của hình ảnh nhúng thủy vân. Kết quả thu được ở hình 8. Như mong đợi, 3 đồ thị tịnh tiến lại gần nhau hơn thử nghiệm ban đầu. Điều đó khiến miền giao nhau lớn hơn và làm việc chọn ngưỡng trở nên khó khăn. Từ đó rút ra được hệ thống này không thể chịu được nhiễu.



Hình 8 Giá trị phát hiện hình ảnh nhúng thủy vân sau khi thêm nhiễu

# 6. Kỹ thuật thủy vân với thông tin bên lề

Nhược điểm của việc không khai thác thông tin bên lề đã được chỉ ra trong hệ thống **blind embedding** ở phần 5. Sự bền bỉ và hiệu quả của quá trình thủy vân có thể được cải thiện rất nhiều bằng cách tận dụng nội dung hình ảnh trong quá trình nhúng. Mô hình chung của các hệ thống sử dụng kỹ thuật thủy vân khai thác thông tin bên lề được miêu tả ở hình dưới.



Hình 9 Dạng chuẩn của các mô hình thủy vân với thông tin bên lề

Sự khác biệt duy nhất giữa mô hình này và mô hình ở phần 5 là việc sử dụng hình ảnh gốc. Khi thực hiện nhúng thủy vân, chương trình mã hóa thông điệp không chỉ sử dụng khóa thủy vân mà còn sử dụng thông tin của ảnh gốc. Thông điệp được mã hóa sau đó được thêm vào ảnh gốc giống như trường hợp không có thông tin bên lề. Trong quá trình truyền, kênh truyền sẽ gia tăng nhiễu lên thông tin, và chương trình nhận diện thủy vân số sẽ cố gắng lấy lại thông điệp ban đầu bằng cách sử dụng khóa thủy vân và thuật toán phát hiện.

Để minh họa việc sử dụng thủy vân số thông tin bên lề, chúng ta sẽ tìm hiểu hai hệ thống. Đầu tiên là hệ thống **blind embedding** mở rộng, trong khi ví dụ còn lại dựa trên mã hóa **dirty paper** - một lớp thuật toán thủy vân phổ biến.

## 6.1 Informed embedding và bộ phát hiện sử dụng tương quan tuyến tính

Hệ thống này thực chất là mở rộng của hệ thống **blind embedding**. Nhằm mục đích mang lại hiệu quả 100% trong việc phát hiện thủy vân, hệ thống kiểm soát giá trị của tham số α - điều đã được chứng minh là cực kì quan trọng. Hệ thống này cũng là một hệ thống thủy vân 1 bit. Thuật toán cho bộ nhúng và bộ dò như sau.

**Bộ nhúng**:

1. Chọn một mẫu tham chiếu ngẫu nhiên. Đây đơn giản là một mảng với số chiều bằng với ảnh gốc, có các phần tử được lấy ngẫu nhiên theo phân phối Gauss trong khoảng [-1, 1]. Khóa thủy vân chính là “hạt giống” được dùng cho việc khởi tạo trình sinh số giả ngẫu nhiên, để tạo ra mẫu tương quan ngẫu nhiên.

2. Tính toán một mẫu thông điệp tùy thuộc vào việc nhúng bit 0 hay 1. Nếu là bit 1, giữ nguyên mẫu tương quan ngẫu nhiên. Còn nếu là bit 0, lấy giá trị âm của mẫu tương quan để thu được mẫu thông điệp.

3. Tính hằng số α bằng cách sử dụng tương quan tuyến tính giữa hình ảnh nhúng thủy vân và mẫu thông điệp. Mục tiêu nhằm đảm bảo giá trị tương quan tuyến tính được sử dụng để phát hiện thủy vân là hằng số và lớn hơn ngưỡng phát hiện. Ta thay thế giá trị này vào vế trái của phương trình tương quan tuyến tính và giải ra α. Bằng cách này, ta có các giá trị α khác nhau với mỗi hình ảnh khác nhau.

4. Nhân mẫu thông điệp với hằng số α để kiểm soát cường độ nhúng.

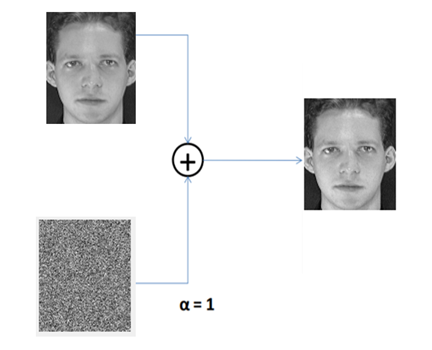
5. Thêm mẫu thông điệp sau khi nhân vào hình ảnh gốc để nhận được hình ảnh nhúng thủy vân.

**Bộ dò**:

1. Tính toán tương quan tuyến tính giữa hình ảnh nhúng thủy vân nhận được và mẫu tương quan ban đầu có thể tạo lại nhờ “hạt giống” khởi tạo được dùng như khóa thủy vân.

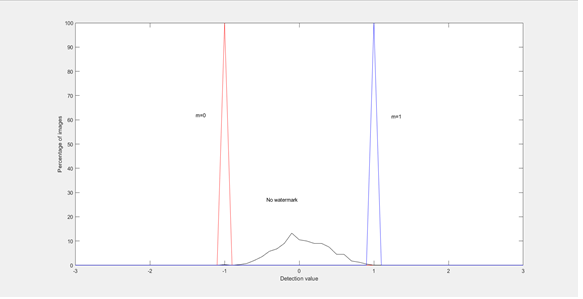
2**.** Quyết định thông điệp thủy vân là gì dựa trên kết quả của sự tương quan. Nếu giá trị tương quan tuyến tính vượt qua ngưỡng, ta sẽ coi thông điệp là 1. Nếu tương quan tuyến tính nhỏ hơn phần âm của ngưỡng ta sẽ coi thông điệp là 0. Nếu tương quan tuyến tính nằm giữa phần âm và phần dương của ngưỡng, coi như không có thông điệp được nhúng.

Một ví dụ về quá trình nhúng được thể hiện trong hình 10. Hình ảnh phía trên bên trái là ảnh gốc, hình ảnh phía dưới là mẫu tham chiếu và bên phải là hình ảnh sau khi nhúng thủy vân - ở đây chúng ta nhúng bit 1. Theo kết quả đã thu được, ta thấy có rất ít sự khác biệt về hình thức giữa 2 hình ảnh.



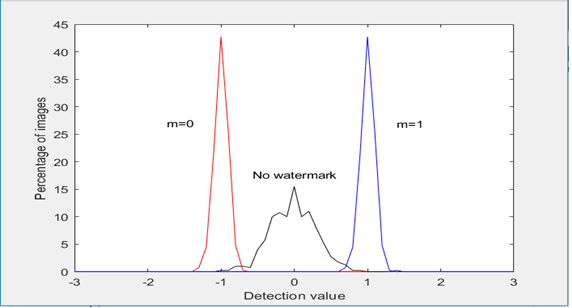
Hình 10 Ví dụ về hình ảnh sau khi nhúng thủy vân

Để kiểm tra tính hiệu quả của hệ thống, ta sử dụng 400 hình ảnh nhỏ (112 x 92 pixel). Ta chạy thuật toán với ngưỡng 0.7 và β = 0.3 (β được thêm vào để dễ dàng vượt ngưỡng) để nhúng bit 1 và 0 vào mỗi hình ảnh, thu được kết quả là 800 hình ảnh được nhúng thủy vân. Sau đó tính toán mối tương quan tuyến tính (như trong bộ dò) cho từng hình ảnh đó, cũng như cho các ảnh gốc (không được nhúng thủy vân) rồi vẽ kết quả. Kết quả được thể hiện ở hình dưới (Hình 11). Trục hoành là giá trị tương quan tuyến tính, trong khi trục tung là tỉ lệ phần trăm của hình ảnh có giá trị tương quan tuyến tính tương ứng.



Hình 11 Giá trị phát hiện cho ảnh sử dụng kỹ thuật thủy vân

Rõ ràng từ hình vẽ, ta thấy ba biểu đồ đại diện cho hình ảnh khi ta nhúng 1 bit 1 hoặc 0, hoặc không có thủy vân được nhúng vào. Ba biểu đồ đó tách biệt và không có sự chồng chéo giữa chúng. Điều này xảy ra là do giá trị của α được điều chỉnh động để tạo ra hình ảnh thủy vân với giá trị phát hiện là 1.0 (0.7 là ngưỡng, cộng với 0.3 vượt ngưỡng của β). Do đó, những hình ảnh đã được nhúng bit 1 có giá trị phát hiện là 1 và những hình ảnh được nhúng bit 0 có giá trị phát hiện là -1. Các giá trị phát hiện của hình ảnh gốc tập trung xung quanh 0 và biểu đồ này về cơ bản giống với giá trị được tạo bởi thử nghiệm ban đầu trong hệ thống nhúng mù. Lý do tại sao các hình ảnh thủy vân không phải tất cả đều có giá trị phát hiện -1 và 1 như dự kiến là bởi vì thuật toán tìm giá trị phát hiện phải làm việc với các lỗi số được tìm ra trong quá trình làm tròn số thực và phải cắt bỏ các giá trị để chuyển chúng thành số nguyên. Đó là bằng chứng cho thấy hệ thống có hiệu quả 100% và có thể chọn ngưỡng để tỉ lệ phát hiện thủy ấn sai sót gần như bằng 0. Ngay cả khi có các nhiễu được thêm vào, hệ thống vẫn khá mạnh mẽ. Chúng tôi đã sửa đổi thí nghiệm để thêm nhiễu Gauss trong khoảng [-10; 10] cho mỗi pixel của hình ảnh thủy vân, để xem thay đổi trong ba biểu đồ. Kết quả được thể hiện như hình 12.



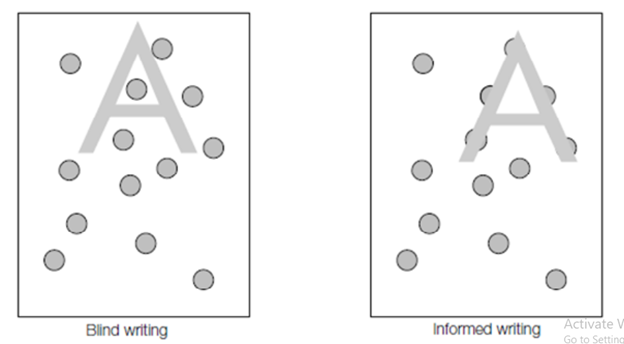
Hình 12 Giá trị phát hiện cho ảnh sử dụng kỹ thuật thủy vân khi thêm nhiễu

Về cơ bản, không có sự khác biệt giữa hình 12 và hình 11, điều này cho thấy sự hiện diện của nhiễu không ảnh hưởng quá nhiều tới các giá trị phát hiện. Do đó, chúng ta có thể kết luận rằng hệ thống này mạnh và kháng nhiễu khá tốt, đây chính là điểm khác biệt so với hệ thống nhúng mù. Nhìn chung, hệ thống nhúng có thông tin hoạt động tốt hơn, cả về hiệu quả và về độ mạnh so với hệ thống nhúng mù.

# 7. Mã Dirty-paper

Mã dirty-paper là một tập hợp của các mã. Trái ngược với mã hóa thông điệp cổ điển (mỗi thông điệp được biểu diễn bằng một từ mã duy nhất), trong một mã dirty-paper mỗi thông điệp được biểu diễn bởi một tập các từ mã. Để truyền tải một thông điệp, bộ mã hóa cần tìm từ mã phù hợp nhất với tín hiệu mà thông điệp được nhúng trong đó. Do đó, đối với mỗi thông điệp, chúng ta có một tập hợp các từ mã, được gọi là “sub-code book”. Sự kết hợp của các “sub-code book” này chính là mã dirty-paper. Các bộ giải mã ở đầu kia của đường truyền cần tìm từ mã gần nhất với tín hiệu nhận được. “Sub-code” chứa từ mã này sau đó được sử dụng để phân loại thông điệp ban đầu nhúng trong tín hiệu nhận được.

Thuật ngữ dirty-paper được đặt ra trong bài báo của Max Costa “Writing on Dirty  
Paper”. Ý tưởng chính là khi viết một biểu tượng trên một tờ giấy bẩn, nên đặt biểu tượng đó vào các vết bẩn đã có sẵn trên tờ giấy. Điều này được minh họa trong hình bên dưới: cho ví dụ về cách viết ký hiệu A trên một tờ giấy bẩn theo cách blind writing và informed writing. Trong kỹ thuật thủy vân, dirty-paper là hình ảnh bao phủ được biết đến bởi người nhúng nhưng không được biết bởi người giải mã. Sử dụng nhiều mã cho mỗi thông điệp, chúng ta có thể chọn mã tốt nhất cho một hình ảnh cụ thể.



Hình 13 Viết ký hiệu A trên dirty paper bằng blind và informed writing

Chất lượng mã dirty paper dựa trên mật độ của sub-code book và mật độ kết hợp của các sub-code book này. Nếu ta có các sub-code book dày đặc, nhiều khả năng sẽ tìm thấy một từ mã gần hơn với ảnh gốc. Tuy nhiên, điều này cũng có nghĩa là sự kết hợp của các sub-code book cũng sẽ dày đặc, dẫn dến dễ dàng gây ra lỗi khi giải mã bởi vì các sub-code book trở nên gần nhau hơn. Lý tưởng nhất là có được những sub-code book với mật độ dày đặc để cung cấp hình ảnh có độ chân thực tốt hơn, và những sự liên kết thưa thớt của các sub-code book này giúp cung cấp một hệ thống bền chắc hơn. Đây là những yêu cầu mâu thuẫn nhau và ta cần cân bằng chúng.

## 7.1 Hệ thống nhúng dựa trên khối với độ bền cố định – bộ phát hiện sử dụng hệ số tương quan

Hệ thống này là một ứng dụng tương đối đơn giản của mã dirty paper để nhúng một bit (1 hoặc 0) vào một hình ảnh. Nó sử dụng cơ chế nhúng dựa trên khối, có nghĩa là quá trình thủy vân được thực hiện trên các vectơ có số chiều nhỏ hơn được trích xuất bởi việc sử dụng các khối thay vì các pixel trong ảnh. Hệ thống cũng sử dụng nhúng với độ bền cố định, nghĩa là lượng nhiễu tối đa mà thủy vân được nhúng vào hình ảnh được giữ cố định thay vì giữ giá trị tương quan không đổi như trong hệ thống nhúng ở phần 6.1. Bô phát hiện sử dụng hệ số tương quan thay vì tương quan tuyến tính để quyết định thông điệp nào được nhúng vào hình ảnh. Thuật toán cho bộ nhúng và bộ dò của hệ thống này như sau:

**Bộ nhúng:**

1. Tạo hai bộ mẫu tham chiếu, mỗi mẫu có kích thước 8 x 8, một bộ tương ứng với thông điệp 1 và bộ còn lại tương ứng với một thông điệp 0. Kích thước của hai bộ là như nhau và điều này rất quan trọng để bảo vệ chất lượng hình ảnh.

2. Trích xuất một vectơ 64 phần tử từ ảnh gốc bằng cách tìm tổng các khối 8 x 8 từ hình ảnh và sau đó lấy trung bình của khối tổng 8 x 8 thu được.

3. Tìm hệ số tương quan của vectơ đã được trích từ ảnh gốc và mỗi mẫu tham chiếu trong tập tương ứng với thông điệp muốn nhúng. Nếu chúng ta muốn nhúng 1, chúng ta chỉ cần xem xét các mẫu tham chiếu được tạo cho 1, không phải những mẫu được tạo cho 0.

4. Chọn mẫu tham chiếu có hệ số tương quan cao nhất (hầu hết tương tự như hình ảnh gốc) và nhúng nó vào hình ảnh bằng cách sử dụng thuật toán độ bền cố định và chiếu lại nó vào kích thước của ảnh gốc.

**Bộ dò:**

1. Trích xuất một vectơ 64 phần tử từ ảnh nhúng thủy vân bằng cách tìm tổng các khối 8 x 8 từ hình ảnh và sau đó lấy trung bình của khối tổng 8 x 8 thu được.

2. Tìm hệ số tương quan của vectơ trích từ hình ảnh được nhúng thủy vân và từng mẫu tham chiếu trong hai bộ tham chiếu tương ứng với 1 và 0.

3. Sau đó mẫu tham chiếu có hệ số tương quan cao nhất được dùng để phân loại thông điệp thủy vân.

**-** Nếu hệ số tương quan của mẫu tham chiếu này nằm dưới ngưỡng cho trước, hình ảnh không có thủy vân được nhúng.

**-** Nếu mẫu tham chiếu này thuộc tập hợp các mẫu tham chiếu tương ứng với 1 và hệ số tương quan của nó nằm trên ngưỡng cho trước, thông điệp là 1.

**-** Nếu mẫu tham chiếu này thuộc tập hợp các mẫu tham chiếu tương ứng với 0 và hệ số tương quan của nó nằm trên ngưỡng đã cho, thông điệp ban đầu là 0.

# 8. Kết luận

Kỹ thuật thủy vân là một lĩnh vực nghiên cứu tích cực với rất nhiều ứng dụng. Mặc dù nó là một lĩnh vực tương đối mới nhưng nó đã tạo ra các thuật toán quan trọng để ẩn thông điệp vào tín hiệu số. Điều này có thể mô tả bởi nhiều mô hình khác nhau. Hai lớp chính của những mô hình này đã được miêu tả ở trên bài tiểu luận. Đó là mô hình truyền thông và mô hình hình học. Mô hình truyền thông có thể được chia nhỏ hơn thành các mô hình sử dụng thông tin bên lề hoặc không sử dụng chúng. Một hệ thống mẫu đã được sử dụng để minh họa các mô hình không sử dụng thông tin bên lề, và hai hệ thống đã được sử dụng để mình họa mô hình sử dụng thông tin bên lề. Mỗi hệ thống này đều có các ưu nhược điểm khác nhau. Việc lựa chọn hệ thống sử dụng phụ thuộc vào yêu cầu cơ bản của ứng dụng.

Tất nhiên, các ví dụ được cung cấp ở đây chỉ là một mẫu nhỏ trong số rất nhiều cách tiếp cận khác nhau để sử dụng kỹ thuật thủy vân. Một số phương pháp khác chưa được đề cập bao gồm phương pháp hoạt động trong miền tần số, tận dụng hệ số DCT và hệ số sóng con.

# Reference

[1] Cox I, Miller M, Bloom J, Fridrich J, Kalker T (2008) Digital Watermarking and

Steganography Second Edition. Elsevier, 2008

[2] Costa M (1983) Writing on dirty paper. IEEE Transactions in Information Theory,

29:439–441, 1983.