# GIẢI PHÁP BẢO VỆ BẢN QUYỀN ẢNH SỐ DỰA TRÊN KỸ THUẬT KẾT HỢP THUỶ VÂN VÀ MÃ HOÁ TRỰC QUAN

**Giang Ngọc Dân**[*], **Tạ Minh Thanh**‡[*]
[*]Học Viện Kỹ Thuật Quân Sự, 236 Hoàng Quốc Việt, Bắc Từ Liêm, Hà Nội

***Tóm tắt*—Bài báo đề xuất một giải pháp bảo vệ bản quyền ảnh số sử dụng kết hợp hai kỹ thuật đang được quan tâm, đó là kỹ thuật thuỷ vân và kỹ thuật mã hoá trực quan. Trong giải pháp của chúng tôi, thông tin bản quyền (logo bản quyền) sẽ được phân tán thành $n$ mảnh sử dụng lược đồ phân tán $k-out-of-n$, còn gọi là lược đồ phân tán $(k,n)$. Một trong số các mảnh thông tin phân tán sẽ được sử dụng để nhúng vào ảnh số để minh chứng bản quyền của người dùng; $n-1$ mảnh phân tán còn lại sẽ được sử dụng để đăng ký với Cục bản quyền tác giả. Khi xác nhận bản quyền thuộc về người dùng, nhà xác minh chỉ cần trích rút thông tin thuỷ vân từ ảnh số, kết hợp với $k-1$ mảnh phân tán bất kỳ đã được đăng ký từ $n-1$ mảnh phân tán để phục hồi thông tin bản quyền. Kết quả thí nghiệm của phương pháp đề xuất so sánh với phương pháp chỉ dùng thuỷ vân số cho thấy phương pháp của chúng tôi có hiệu quả thực tế hơn trong ứng dụng bảo vệ bản quyền sản phẩm số.**

***Từ khóa*—Thủy vân ảnh kỹ thuật số, Mã hoá trực quan, Bảo vệ bản quyền hình ảnh, Biến đổi sóng con rời rạc (DWT), Biến đổi Cosine rời rạc (DCT), Xác thực bản quyền tác giả.**

## I. GIỚI THIỆU

Cuộc cách mạng công nghiệp 4.0 đã đem lại những thay đổi sâu sắc trong xã hội và trong cuộc sống. Sự ra đời của những phần mềm có tính năng rất mạnh, các thiết bị mới như máy ảnh kỹ thuật số, máy quét chất lượng cao, máy in, máy ghi âm kỹ thuật số, v.v... đã với tới thế giới tiêu dùng rộng lớn để sáng tạo, xử lý và thưởng thức các dữ liệu đa phương tiện (multimedia data). Mạng Internet toàn cầu đã biến thành một "xã hội ảo" nơi diễn ra quá trình trao đổi thông tin trong mọi lĩnh vực như: chính trị, quân sự, quốc phòng, kinh tế, thương mại. Chính trong môi trường mở và tiện nghi như thế đã xuất hiện những vấn nạn, tiêu cực như nạn ăn cắp bản quyền, nạn xuyên tạc thông tin, truy cập thông tin trái phép. Một giải pháp bảo vệ được sản phẩm số, bảo toàn thông tin và bảo vệ bản quyền tác giả cho các sản phẩm số đang được yêu cầu một cách cấp thiết. Trong các giải pháp hiện nay, thuỷ vân số là giải pháp đang được nhiều chuyên gia ủng hộ cho vấn đề bảo vệ bản quyền sản phẩm đa phương tiện.

Để một phương pháp thủy vân kỹ thuật số có hiệu quả thì tính ẩn và tính bền vững trước các thao tác hình ảnh phổ biến như: nén, lọc, xoay, cắt xén theo tỷ lệ, các cuộc tấn công thông đồng trong số nhiều hoạt động xử lý tín hiệu kỹ thuật số khác cần được đảm bảo. Các kỹ thuật thủy vân ảnh kỹ thuật số hiện nay có thể nhóm lại thành hai nhóm chính: kỹ thuật thủy vân miền không gian và kỹ thuật thủy vân miền tần số. So với kỹ thuật thủy vân miền không gian, kỹ thuật thủy vân miền tần số chứng minh sự hiểu quả hơn trong việc đạt được các yêu cầu về tính ẩn và tính bền vững của thuật toán thủy vân kỹ thuật số.

Các biến đổi miền tần số thường được sử dụng bao gồm: Biến đổi sóng con rời rạc (Discrete Wavelet Transform - DWT), Biến đổi Cosine rời rạc (Discrete Consine Tranform - DCT) và Biến đổi Fourier rời rạc (Discrete Fourier Transform - DFT). Những đề xuất sử dụng những biến đổi miền tần số đã được đề cập rất nhiều trong những nghiên cứu gần đây như đề xuất kỹ thuật thuỷ vân trên miền tần số DCT [1]–[4], trên miền tần số DWT [5]–[8], và trên miền tần số DFT [9], [10].

Tác giả liên hệ: Giang Ngọc Dân,
Email: giangngocdan3110@gmail.com.
Đến tòa soạn: 10/2020, chỉnh sửa: 11/2020, chấp nhận đăng: 12/2020.
‡ Corresponding author

Những phương pháp đề xuất này đã chỉ rõ được ưu điểm của việc giấu thông tin trên miền tần số để tạo ra các giải pháp thuỷ vân bền vững, phù hợp cho các ứng dụng bảo vệ bản quyền sản phẩm số. Các kỹ thuật thuỷ vân trên miền tần số thường được lựa chọn cho thích hợp với những đối tượng chịu tác động của các kỹ thuật như nén sẽ được áp dụng cho giải pháp thuỷ vân trên miền tần số DCT, cải tiến chất lượng ảnh sau khi nhúng thuỷ vân sẽ được áp dụng cho giải pháp thuỷ vân trên miền tần số DWT, ... Tuy nhiên, DWT được sử dụng trong thủy vân ảnh kỹ thuật số thường xuyên hơn do đặc tính định vị không gian và đa độ phân giải của nó, tương tự như mô hình lý thuyết của hệ thống thị giác con người. Các cải tiến hiệu năng tốt hơn trong các thuật toán thủy vân ảnh kỹ thuật số dựa trên DWT có thể đạt được bằng nhiều cách cho phù hợp với những đối tượng sản phẩm số khác nhau như nhạc số, phim số, và ảnh số.

Để cân bằng việc cải tiến chất lượng ảnh số sau khi nhúng thuỷ vân và tính bền vững của thông tin thuỷ vân, những nghiên cứu trên miền tần số mở rộng như $q$-DCT [11], $q$-DWT [12], hay $q$ - SVD [13] cũng được đề xuất nhằm cân bằng hai mục tiêu trên. Tuy nhiên, việc điều chỉnh giá trị tham số $q$ để thoả mãn điều kiện cân bằng cả hai tiêu chí là khó đạt được. Các tác giả đã phải thực hiện bước đánh giá khảo sát tiêu chí chất lượng ảnh sau khi nhúng và độ bền vững của thuỷ vân để chọn ra giá trị thích hợp nhất cho tham số $q$.

Một kỹ thuật khác nhằm bảo vệ bản quyền ảnh số là kỹ thuật thuỷ vân rỗng, trong đó, thông tin thuỷ vân sẽ không nhúng trực tiếp vào ảnh số mà các đặc trưng bền vững của ảnh số sẽ được trích chọn để mã hoá với thông tin bản quyền để tạo ra thông tin đăng ký với Cục bản quyền tác giả [14]. Tuy nhiên, thuỷ vân rỗng phụ thuộc nhiều vào tính chất và đặc trưng của ảnh số. Đối với những ảnh có độ "phức tạp" lớn thì đặc trưng được trích rút sẽ bền vững với những tấn công ảnh.

Trong bài báo này, để làm phong phú tính ứng dụng trong sử dụng miền tần số DWT, chúng tôi đề xuất thuật toán thủy vân ảnh kỹ thuật số dựa trên việc kết hợp kỹ thuật mật mã trực quan (Visual Secret Sharing) và phép biến đổi sóng con rời rạc DWT. Điểm nổi bật của thuật toán là thủy vân, còn gọi là thông tin bản quyền, được chia thành các mảnh chia sẻ bí mật (shares) bằng kỹ thuật mật mã trực quan, sau đó được nhúng vào các băng con DWT đã được lựa chọn của ảnh chứa thông tin. Việc xác định bản quyền sản phẩm số được thực hiện trong việc trích thông tin từ ảnh số, đồng thời phải kết hợp với giải mã trong mật mã trực quan để phục hồi lại thông tin bản quyền. Chính vì vậy, tính bảo mật thông tin bản quyền tác giả cũng được cải thiện và đảm bảo an toàn cho người sử dụng.

Trong bài báo này, chúng tôi tổ chức nội dung như sau: Các kiến thức liên quan được trình bày trong mục II. Trong mục III, kiến trúc và chi tiết mô tả về mô hình đề xuất được đưa ra. Thí nghiệm và đánh giá được trình bày trong phần IV. Kết luận, dự kiến nội dung cải thiện và xu hướng nghiên cứu được đưa ra trong mục V.

## II. CÁC KỸ THUẬT LIÊN QUAN

Phép biến đổi DWT đã được sử dụng rộng rãi trong nhiều ứng dụng xử lý tín hiệu kỹ thuật số. Trong khi đó, kỹ thuật mật mã trực quan là một kỹ thuật mã hóa mà ở đó thông tin trực quan (hình ảnh, văn bản,...) được mã hóa sao cho việc giải mã có thể được thực hiện bởi hệ thống thị giác của con người. Trong phần này, chúng tôi giới thiệu ngắn gọn hai kỹ thuật trên và phác họa liên quan của chúng đối với việc triển khai kỹ thuật thủy vân trên ảnh kỹ thuật số.

### *A. Biến đổi DWT*

Biến đổi DWT: Sóng con là các hàm đặc biệt ở dạng tương tự như hình sin và cosin trong phân tích Fourier, được sử dụng như các hàm cơ sở để biểu diễn tín hiệu [21]–[24].

Do nhu cầu tính toán và xử ly các dữ kiện thực trên máy tính, Daubechies (1990) đưa ra một một họ Wavelet quan trọng được dùng để tính biến đổi Wavelet rời rạc (DWT). Theo cách tiếp cận này, ứng với hàm Wavelet $\Psi(x)$, người ta đưa ra một hàm số tỉ lệ $\Phi(x)$ được dùng để tính $\Psi(x)$ . Mối quan hệ giữa hàm tỉ lệ và hàm wavelet được cho bởi công thức (1) và (2):

$$\Phi(x) = \sum_{k=0}^{N-1} c_k \phi(2x - k) \quad (1)$$

$$\Psi(x) = \sum_{k=0}^{N-1} (-1)^k c_k . \Phi(2x + k - N + 1) \quad (2)$$

Với Φ(x) là hàm tỉ lệ, Ψ(x) là hàm Wavelet, $N$ là một số chẵn và $k \in Z$.

Các phép lọc được tiến hành với nhiều tầng (level) khác nhau và để khối lượng tính toán không tăng, khi qua mỗi bộ lọc, tín hiệu được lấy mẫu xuống 2.

Ứng với mỗi tầng, tín hiệu có độ phân giải khác nhau. Do đó, phép biến đổi sóng con rời rạc được gọi là phân tích đa phân giải (MRA - Multiresolution Analysis).

Tại mỗi tầng lọc, biểu thức của phép lọc được cho bởi công thức (3) và (4):

$$y_{high}(n) = \sum_n S(n).g(2k-n), \tag{3}$$

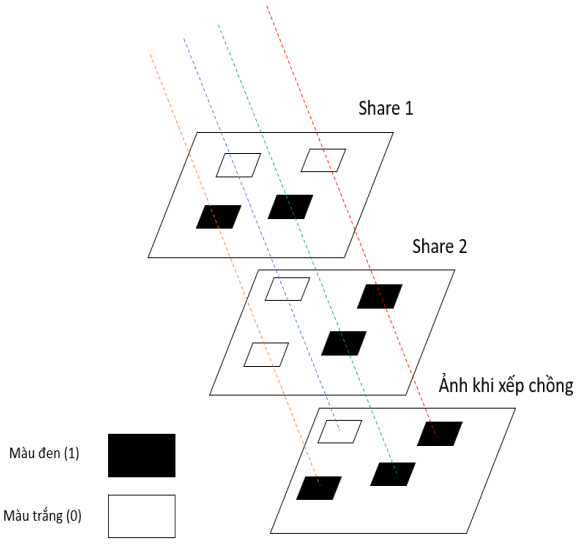
$$y_{low}(n) = \sum_n S(n).h(2k-n), \tag{4}$$

trong đó, $S(n)$ là tín hiệu, $h(n)$ là đáp ứng xung của các bộ lọc thông thấp tương ứng với hàm (1) và $g(n)$ là đáp ứng xung của các bộ lọc thông cao tương ứng với hàm (2). Hai bộ lọc này liên hệ nhau theo hệ thức (5):

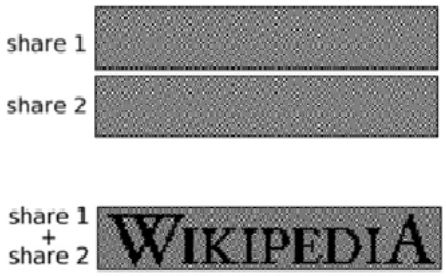
$$h(N-1-n) = (-1)^n g(n), \tag{5}$$

trong đó, $N$ là số mẫu trong tín hiệu.

Tín hiệu $S(n)$ có thể được tái tạo theo các bước ngược lại gọi là phép biến đổi sóng con rời rạc nghịch (IDWT, inverse discrete wavelet transform).




Hình 1: Hệ thống thị giác của con người có chức năng như một phép OR




Hình 2: Ví dụ cho lược đồ chia sẻ bí mật của Shamir

### *B. Mật mã trực quan - Visual Secret Sharing*

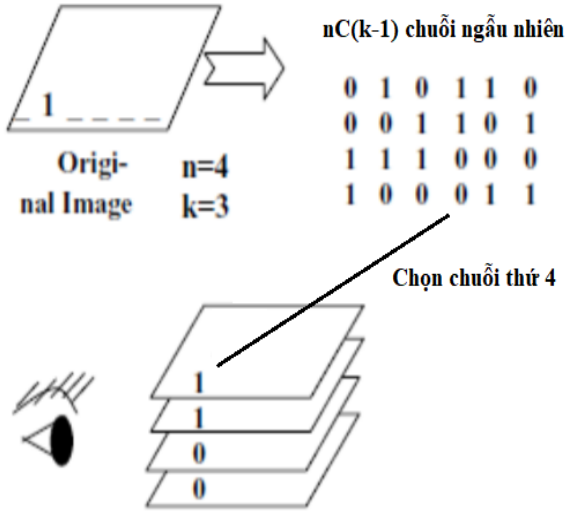
Mật mã trực quan là một kỹ thuật mã hóa mà trong đó, thông tin trực quan (hình ảnh, văn bản...) được mã hóa theo cách mà việc giải mã có thể được thực hiện thông qua hệ thống thị giác của con người (Hình 1) mà không cần đến sự trợ giúp của máy tính [15].

Ý tưởng của chia sẻ bí mật được đề xuất bởi Adi Shamir [16] và G.Blakley [17] vào năm 1979. Bốn năm sau đó, vào năm 1983, một phương pháp chia sẻ bí mật khác được để xuất bởi Asmuth và Bloom [18]. Theo đó, lược đồ của Shamir dựa trên phép nội suy đa thức; lược đồ của Blakley dựa trên hình học siêu phẳng và lược đồ của Asmuth và Bloom dựa trên định lý số dư Trung Quốc.

Trong số những lược đồ chia sẻ bí mật được đề xuất, lược đồ chia sẻ bí mật của Shamir được xem là tiềm năng nhất cho việc bảo vệ bản quyền hình ảnh. Nền tảng của lược đồ này là chia hình ảnh thành các mảnh chia sẻ bí mật (shares hay shadows). Để thu được hình ảnh gốc, chúng ta chỉ cần kết hợp các shadows này lại với nhau như Hình 2.

Trong bài báo này, chúng tôi sử dụng phương pháp tạo các mảnh chia sẻ bí mật từ hình ảnh gốc (Original Image) bằng "Chuỗi ngẫu nhiên" - $RandomSequence$ [19]. Với lược đồ $k-out-of-n$, giả sử, ta có một tập **P** của $n$ phần tử, một hình ảnh bí mật **S** được mã hóa trong $n$ phần tử này được gọi là các mảnh chia sẻ bí mật. Với mỗi một thành phần trong tập **P** sẽ nhận một mảnh chia sẻ, với bất kỳ $k$ mảnh chia sẻ hoặc nhiều hơn được xếp chồng lên nhau thì thông điệp (hình ảnh) sẽ được hiển thị. Nhưng nếu có ít hơn $k$ mảnh chia sẻ hoặc cố gắng phân tích bằng một phương pháp khác thì thông điệp đó vẫn được mã hóa.

Đối với lược đồ $k-out-of-n$ sử dụng *Chuỗi*




Hình 3: Chuỗi ngẫu nhiên

*ngẫu nhiên - Random Sequence*, một chuỗi ngẫu nhiên được cấu thành từ $(n-k+1)$ giá trị "1" và $(k-1)$ giá trị "0". Trong lược đồ này, chúng ta sẽ có số lượng chuỗi ngẫu nhiên $(ns)$ là tổ hợp chập $(k-1)$ của $n$ (**ns = nC(k - 1)**).

Khi tiến hành tạo các mảnh chia sẻ bí mật, trước tiên, chúng tôi khởi tạo toàn bộ các bit của $n$ mảnh chia sẻ bí mật bằng "0", sau đó chuyển giá trị của tất cả các điểm ảnh trên ảnh gốc $I$ thành các bit nhị phân. Tại mỗi điểm ảnh trên $I$, xác định vị trí của các bit có giá trị bằng "1". Nếu bit ở vị trí đã xác định có giá trị bằng "1" thì cũng tại vị trí bit đó trên $(n-k+1)$ mảnh chia sẻ bí mật của tập hợp $n$ mảnh chia sẻ cũng phải được gán giá trị "1" và cũng ở vị trí đó trên $(k-1)$ mảnh chia sẻ còn lại sẽ mang giá trị "0". Nếu nhìn từ một phía khi xếp chồng các mảnh chia sẻ với nhau thì chuỗi bit ở vị trí được xác định sẽ có $(n-k+1)$ số "1" và $(k-1)$ số "0". Điều này được mô tả trực quan như Hình 3.

Các bước tiến hành tạo các mảnh chia sẻ bí mật bằng chuỗi ngẫu nhiên *Random Sequence* như sau:

**Bước 1:** Đưa vào ảnh gốc logo $I$, số mảnh chia sẻ cần tạo $(n)$ và số mảnh chia sẻ tối thiểu để tái tạo lại ảnh gốc $(k)$.

**Bước 2:** Tính số lượng chuỗi ngẫu nhiên (**ns**). Với *ns = nC(k-1)* và khởi tạo các chuỗi ngẫu nhiên: $Sq_1, Sq_2, ..., Sq_{ns}$.

**Bước 3:** Giả sử các mảnh chia sẻ của ảnh gốc $(I)$ được ký hiệu là $S_1, S_2, ..., S_n$ và được tạo ra bởi logic sau:

+ Khởi tạo tất cả các bit của $S_t$ là giá trị "0", với $(1 \leq t \leq n)$.

+ Nếu bit thứ $i$ của một điểm ảnh trên $I$ mang giá trị "1" thì:

*Tạo một số ngẫu nhiên $r$ trong khoảng từ 1 đến **ns**.*

*Tiến hành phép tính toán **OR** giữa bit thứ $i$ của $S_j$ (Với $1 \leq j \leq n$) với bit thứ $j$ của chuỗi $Sq_r$, với $1 \leq r \leq ns$.*

Các bước tiến hành tái tạo hình ảnh ban đầu:

**Bước 1:** Chọn $s$ mảnh chia sẻ (với $s \geq k$ ) trong số $n$ mảnh chia sẻ bí mật được tạo ra trước đó.

**Bước 2:** Tiến hành phép **OR** giữa các bit thứ $j$ của các mảnh chia sẻ với nhau. Với $1 \leq j \leq w*h$ để phục hồi hình ảnh logo $I$ với kích thước $w \times h$.

Với việc áp dụng thuật toán của VSS như trên, chúng tôi có thể phân tán ảnh logo là thông tin bản quyền để có thể cải thiện tính bảo mật thông tin tác giả khi nhúng thông tin bản quyền vào sản phẩm số.

### *C. Một số kỹ thuật bảo vệ bản quyền ảnh số*

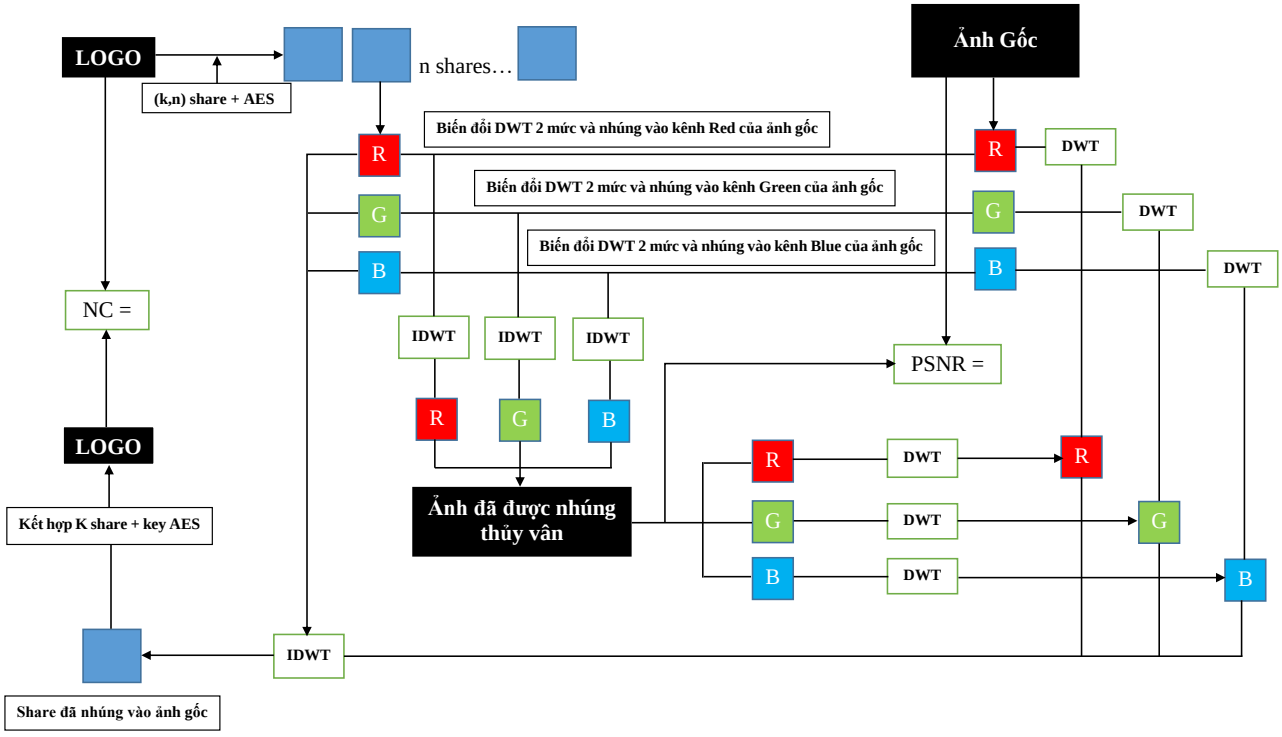
Để bảo vệ được bản quyền tác giả của các sản phẩm số, các kỹ thuật bảo vệ phải đảm bảo được sản phẩm đó mang những thông tin đặc biệt, như thông tin tác giả, ngày sinh, ... nhằm chứng minh được với mọi người sản phẩm đó thuộc quyền sở hữu của người tạo ra sản phẩm số.

Dựa trên yêu cầu đó, một số giải pháp bảo vệ bản quyền ảnh số đã được đề xuất như:

***Thủy vân số***: Đây không phải là một kỹ thuật mới, phương pháp thủy vân đầu tiên được tiến hành trên giấy với mục đích truyền tin mật. Đó là một thông tin nhỏ được nhúng chìm trong giấy để thể hiện bản gốc của mẩu tin.

Đối với thủy vân trên ảnh số, kỹ thuật nhúng một lượng thông tin vào bức ảnh và thông tin đó sẽ gắn liền với bức ảnh. Điều đó có nghĩa là, thông tin sau khi được nhúng vào bức ảnh nó sẽ trở thành một thành phần của bức ảnh đó. Chính vì yếu tố này mà thủy vân trên ảnh số được áp dụng rất phổ biến cho mục đích bảo vệ bản quyền ảnh số.

***Mã hóa***: Các kỹ thuật mã hóa đối với vấn đề bảo vệ bản quyền ảnh số, là hoàn toàn khác so với thủy vân. Mã hóa cung cấp phương thức bảo mật thông qua việc mã hóa và giải mã. Tuy nhiên,




Hình 4: Sơ đồ mô tả thuật toán

mã hóa không thể cung cấp khả năng giám sát và bảo vệ nội dung thông tin sau khi giải mã.

Ngoài ra, việc tấn công trên hệ thống mã hóa và hệ thống thủy vân cũng có nhiều khác biệt. Đối với mã hóa, khi kẻ tấn công giải mã được thông điệp bí mật cũng tức là hệ thống mã hóa đã bị phá vỡ. Nhưng để phá vỡ một hệ thống thủy vân cần hai giai đoạn là: kẻ tấn công phải phát hiện được kỹ thuật thủy vân đang được sử dụng, hai là, kẻ tấn công phải đọc, sửa đổi hoặc loại bỏ được thủy vân đã được nhúng.

Như vậy, kỹ thuật thủy vân và mã hóa, cả hai đều có những ưu và nhược điểm riêng, do đó, trong nhiều trường hợp nên sử dụng kết hợp cả hai kỹ thuật này. Ở phần tiếp theo của bài báo này, chúng tôi sẽ đề xuất một giải pháp kết hợp giữa thủy vân và mã hóa nhằm đảm bảo cả hai yếu tố bảo mật thông tin và bảo vệ được bản quyền tác giả cho ảnh số.

## III. ĐỀ XUẤT THUẬT TOÁN BẢO VỆ BẢN QUYỀN ẢNH SỐ KẾT HỢP THUỶ VÂN VÀ VSS

Trong bài báo này, chúng tôi tập trung nghiên cứu về thuật toán nhúng và trích thủy vân đối với ảnh màu (color image) sử dụng phép biến đổi sóng con DWT. Dữ liệu đầu vào của thuật toán là: 01 ảnh màu để làm ảnh chứa thủy vân (Cover Image) và 01 ảnh màu khác để làm logo (Secret Image). Để tăng mức độ bảo mật cho thủy vân, chúng tôi sử dụng kỹ thuật mật mã trực quan để chia ảnh thủy vân thành $n$ mảnh chia sẻ bí mật. Một trong số $n$ mảnh chia sẻ bí mật được tạo ra sẽ được chọn làm ảnh thủy vân (Watermark) và được nhúng vào ảnh chứa thủy vân. Kỹ thuật nhúng thuỷ vân của bài báo sẽ được triển khai trên cả ba kênh màu R, G, B của ảnh gốc sau khi biến đổi tần số DWT.

Để xác minh bản quyền tác giả của ảnh số, sau khi trích xuất thủy vân (mảnh chia sẻ bí mật đã được nhúng vào ảnh chứa), tiếp tục áp dụng kỹ

thuật mật mã trực quan để tổng hợp các mảnh chia sẻ để thu được logo ban đầu.

Sơ đồ quy trình hoạt động của thuật toán được mô tả trong Hình 4.

### A. *Thuật toán nhúng thuỷ vân*

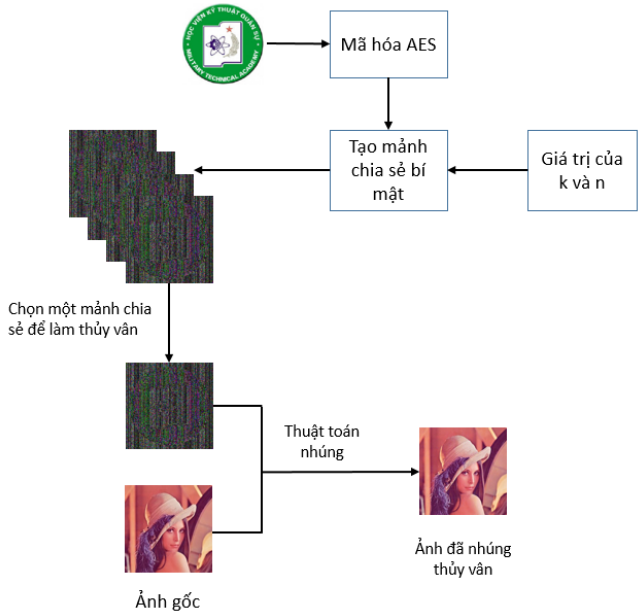
Hình 5 mô tả hệ thống đề xuất của chúng tôi kết hợp kỹ thuật mật mã trực quan vào quá trình nhúng thủy vân. Thuật toán nhúng thủy vân dựa trên phương pháp biến đổi sóng con rời rạc đối với ảnh màu kết hợp với kỹ thuật mật mã trực quan giúp nâng cao nhiều khả năng ứng dụng mới trong lĩnh vực bảo vệ bản quyền tác giả.

Sau khi áp dụng kỹ thuật mật mã trực quan để tạo $n$ mảnh chia sẻ bí mật từ ảnh logo, chọn một hoặc một số mảnh chia sẻ và nhúng vào ảnh chứa. Quá trình nhúng thủy vân vào ảnh chứa được mô tả như Hình 6.

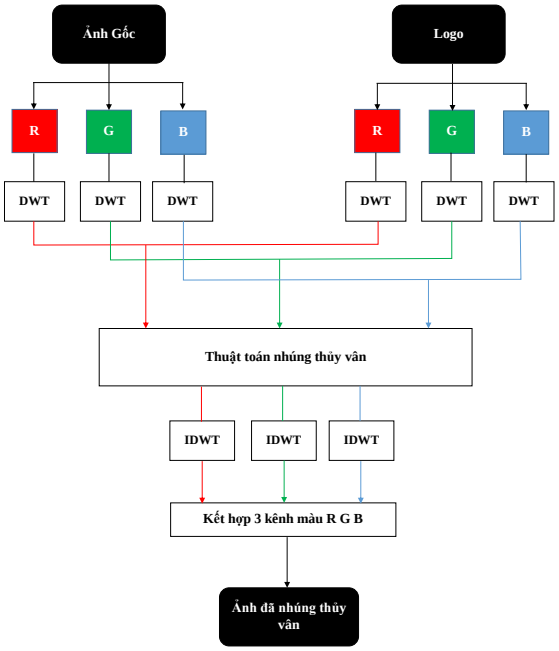
**Bước 1:** Tiến hành tách ảnh gốc và ảnh logo thành các kênh màu riêng biệt Red (R), Green (G), Blue (B).

**Bước 2:** Áp dụng DWT để phân tích ảnh gốc thành bốn băng con: LL1, HL1, LH1 và HH1. Tiếp tục biến đổi DWT cho băng con HL1 để có bốn các băng con nhỏ hơn và chọn băng con LL2.

**Bước 3:** Thực hiện nhúng thủy vân trên từng




Hình 5: Mô tả việc ứng dụng mật mã trực quan vào thuật toán




Hình 6: Thuật toán nhúng thủy vân sử dụng DWT

kênh màu theo công thức sau:

$$Watermarked_{i,j} = V_{i,j} + \alpha W_{i,j}, \qquad (6)$$

trong đó:

$Vi, j$ là băng con với hệ số tương ứng.

$\alpha$ là cường độ nhúng trên từng kênh màu.

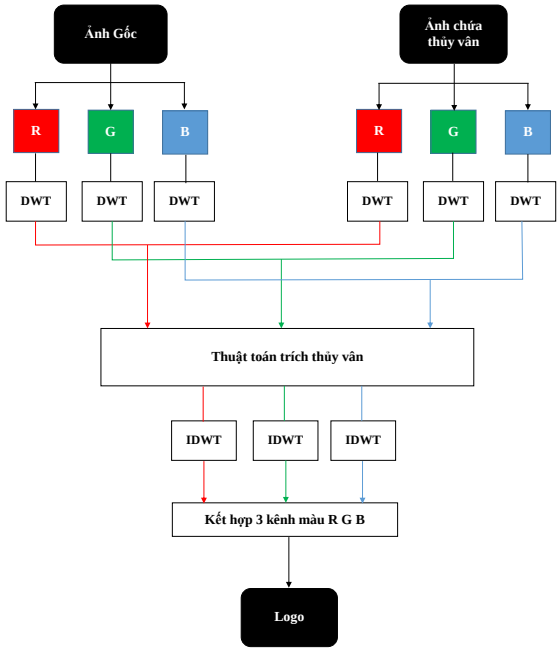
**Bước 4:** Thực hiện phép biến đổi IDWT 2 mức và kết hợp các kênh màu để thu được ảnh đã nhúng thủy vân.

### B. *Thuật toán trích xuất thủy vân*

Quá trình trích rút thông tin thực hiện ngược lại so với quy trình nhúng thông tin, được mô tả trong Hình 7.

**Bước 1:** Tiến hành phân tích ảnh gốc và ảnh đã thủy vân thành các kênh màu riêng biệt Red (R), Green (G), Blue (B).

**Bước 2:** Thực hiện phép biến đổi DWT 2 mức cho ảnh chứa thủy vân và ảnh gốc.




Hình 7: Thuật toán trích rút thủy vân sử dụng DWT

**Bước 3:** Tiến hành trích xuất thủy vân theo công thức sau:

$$Extracted_{i,j} = (W_{i,j} - V_{i,j})/\alpha, \qquad (7)$$

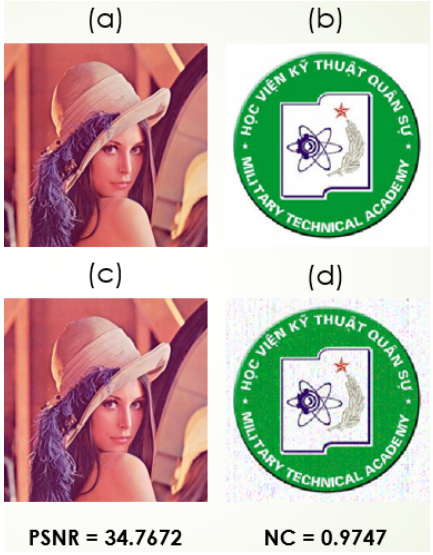
trong đó, $W_{i,j}$ và $V_{i,j}$ là thành phần LL2 của ảnh đã giấu thuỷ vân và ảnh gốc. $Extracted_{i,j}$ là thành phần của thuỷ vân trích rút.

**Bước 4:** Tái tạo ảnh logo ban đầu bằng cách kết hợp thủy vân vừa trích xuất được với các mảnh chia sẻ bí mật thu được ở phần mật mã trực quan.

## IV. Kết quả thực nghiệm và khảo sát

Ở mục này, chúng tôi sử dụng hình ảnh Lena, Pepper, Couple, Mandrill, Parrots kích thước $256 \times 256$ để làm ảnh chứa thủy vân và ảnh logo của Học viện Kỹ thuật quân sự để làm thủy vân, nhằm đánh giá hiệu năng của thuật toán thủy vân trên miền tần số DWT kết hợp kỹ thuật mật mã trực quan để đánh giá và thử nghiệm mô hình đề xuất.

Hiệu quả của thuật toán thường được đánh giá bởi hai đặc trưng là: tính không thể nhận biết được và tính bền vững.




Hình 8: Ảnh gốc (a), Logo gốc (b), Watermarked Image (c), Thủy vân trích xuất được (d)

Bảng I: Kết quả PSNR và NC trên các ảnh chứa khác nhau

| Ảnh thử nghiệm | PSNR | NC |
|---|---|---|
| Lena | 34.7672 | 0.974729 |
| Pepper | 34.7935 | 0.975822 |
| Couple | 34.8068 | 0.975416 |
| Mandrill | 34.8077 | 0.976204 |
| Parrots | 34.9288 | 0.973707 |

### A. Tính không thể nhận biết được

Được định nghĩa là chất lượng cảm nhận của hình ảnh mang tin không được làm biến dạng bởi sự hiện diện của ảnh thủy vân. Để đánh giá chất lượng của hình ảnh có chứa thủy vân, sử dụng tỷ số tín hiệu cực đại trên nhiễu (Peak signal to noise ratio - PSNR). PSNR tính băng đơn vị decibel (dB) được đưa ra trong công thức (8) dưới đây:

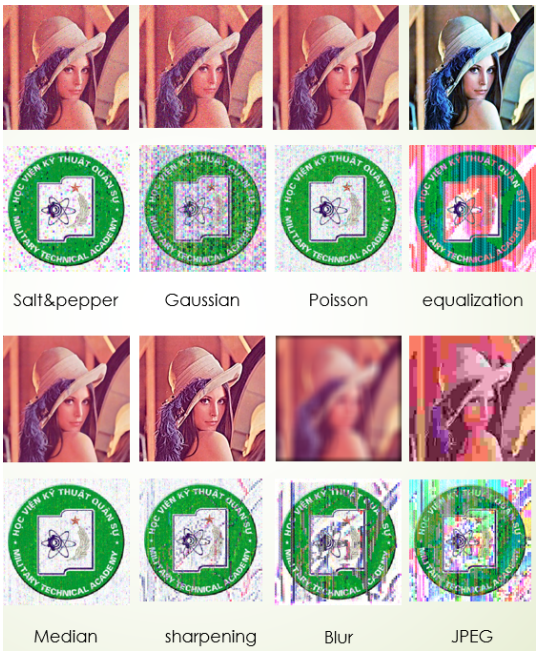
$$PSNR = 20\log_{10}\frac{MAX(I)}{\sqrt{MSE}}, \qquad (8)$$

trong đó, $MAX(I) = 255$ và giá trị của MSE được tính bởi công thức (9):

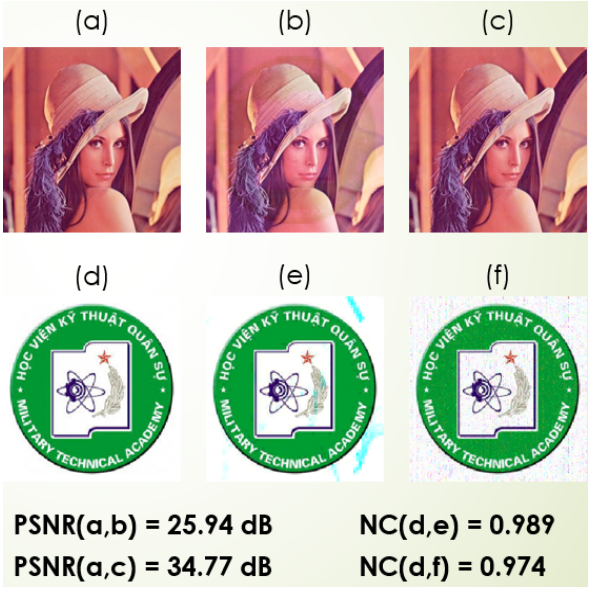
$$MSE = \frac{1}{pxq}\sum_{i=1}^{p}\sum_{j=1}^{q}(I(i,j) - I_w(i,j))^2 \qquad (9)$$

### B. Tính bền vững

Tính bền vững là thước đo khả năng miễn nhiễm của thủy vân trước các loại tấn công khác nhau. Để đánh giá tính bền vững của thủy vân




Hình 9: Kết quả trích xuất thủy vân sau khi thử nghiệm tấn công




Hình 10: Ảnh gốc (a), Watermarked không phân tán (b) và phân tán (c), Thủy vân gốc (d), thủy vân không phân tán (e) và phân tán (f)

Bảng II: Giá trị NC khi sử dụng phương pháp được đề xuất trên ảnh chứa Lena trong điều kiện bị tấn công

| Loại tấn công | NC |
|---|---|
| salt and pepper | 0.92044 |
| gaussian | 0.82326 |
| poisson | 0.91805 |
| equalization | 0.70237 |
| median | 0.9567 |
| sharpening | 0.95019 |
| blur | 0.8814 |
| JPEG | 0.78889 |

trong điều kiện bị tấn công, chúng tôi sử dụng hệ số tương quan chéo chuẩn hóa NC (Normalization Cross - Correlation), được tính bởi công thức dưới đây:

$$NC = \frac{\sum_{i=1}^{M_1}\sum_{j=1}^{M_2} W(i,j).W'(i,j)}{\sum_{i=1}^{M_1}\sum_{j=1}^{M_2}, W(i,j)^2} \qquad (10)$$

trong đó, $W(i,j), W'(i,j)$ là giá trị của các phần tử của logo gốc và logo sau khi phục hồi. Hệ số tương quan chéo chuẩn hóa NC, có giá trị trong khoảng từ 0 đến 1. Giá trị của NC càng gần với 1, tính bền vững của giải pháp thuỷ vân càng tốt. Tuy nhiên, với NC lớn hơn hoặc bằng 0.75 là ngưỡng có thể chấp nhận được.

### *C. Các phép tấn công ảnh*

Dựa vào những biến đổi có chủ đích hay không có chủ đích đối với hệ thủy vân mà ta có thể phân biệt thành một số loại tấn công sau:

- Biến đổi tín hiệu: làm sắc nét, thay đổi độ tương phản, màu, gamma.
- Nhiễu cộng, nhiễu nhân.
- Lọc tuyến tính.
- Nén mất thông tin.
- Giảm dữ liệu: cropping, sửa histogram.
- Thủy vân nhiều lần.

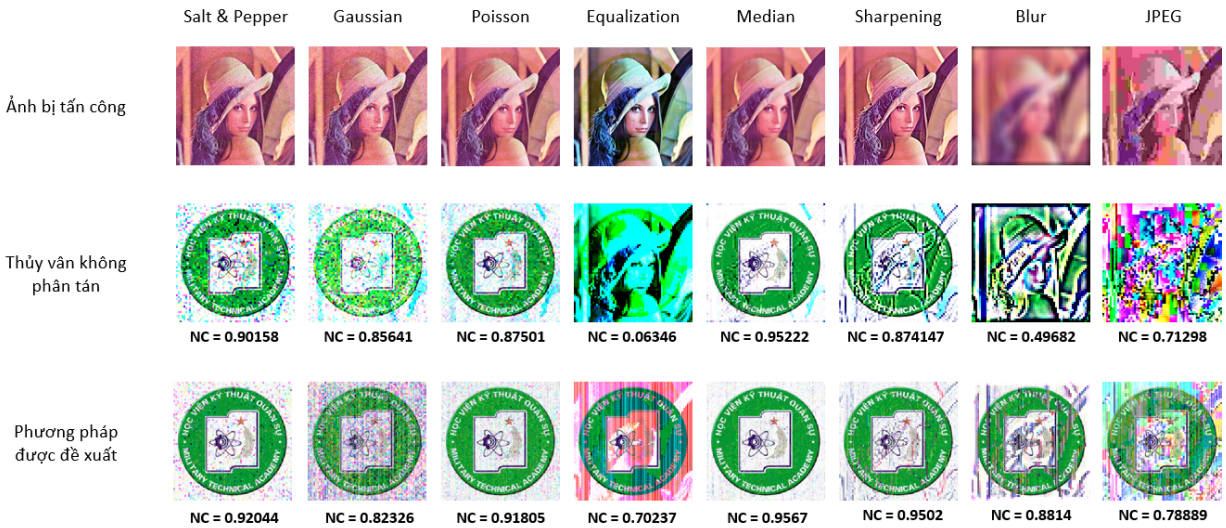
Trong bài báo này, chúng tôi sẽ tiến hành thử nghiệm tấn công trên ảnh đã nhúng thuỷ vân và đánh giá kết quả về hiệu quả của thuật toán trước một số loại tấn công như: nhiễu salt and pepper, làm mờ ảnh, lọc trung bình và thay đổi độ tương phản, ...

### *D. Kết quả thực hiện*

Chúng tôi thực hiện thuật toán mật mã trực quan cho hình "logo" như đã đề cập ở phần trước để thu được các mảnh chia sẻ bí mật, sau khi được mã hóa qua kỹ thuật mật mã trực quan thủy vân được gọi là thủy vân phân tán, sau đó áp dụng phép biến đổi sóng con rời rạc DWT 2 mức cho 5 ảnh màu và chọn một mảnh chia sẻ bí mật để nhúng vào băng con LL2 của mỗi ảnh.

Bảng III: Đánh giá kết quả NC giữa phương pháp thủy vân được đề xuất và phương pháp thủy vân không phân tán trong điều kiện bị tấn công

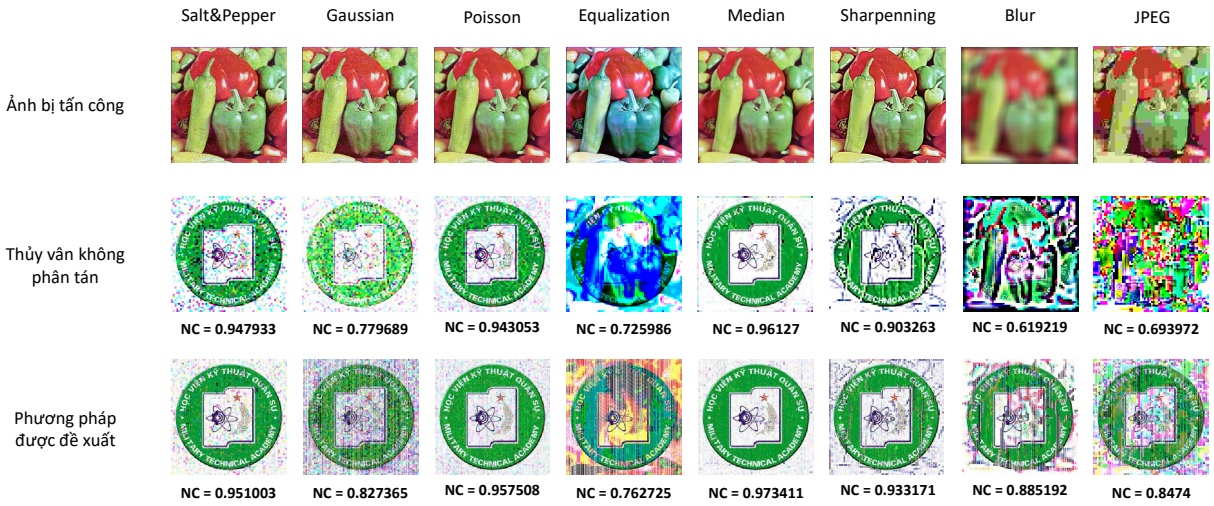
| Loại tấn công | Lena | | Pepper | | Couple | | Mandrill | | Parrots | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Không phân tán | **Đề xuất** | Không phân tán | **Đề xuất** | Không phân tán | **Đề xuất** | Không phân tán | **Đề xuất** | Không phân tán | **Đề xuất** |
| Salt and pepper | 0.90158 | **0.92044** | 0.94793 | **0.95103** | 0.9316 | **0.99298** | 0.93381 | **0.95273** | 0.93565 | **0.94549** |
| Nhiễu Gaus-sian | 0.85641 | **0.82326** | 0.77968 | **0.82737** | 0.61476 | **0.79696** | 0.83546 | **0.98768** | 0.83709 | **0.88191** |
| Nhiễu Poisson | 0.87501 | **0.91805** | 0.94305 | **0.95751** | 0.95824 | **0.97769** | 0.93233 | **0.94267** | 0.93043 | **0.94571** |
| Equaliz ation | 0.06346 | **0.70237** | 0.72598 | **0.7627** | 0.58557 | **0.50587** | 0.56728 | **0.84345** | 0.71602 | **0.78542** |
| Lọc Median | 0.95222 | **0.9567** | 0.96127 | **0.9734** | 0.96353 | **0.97186** | 0.93928 | **0.9477** | 0.96776 | **0.97002** |
| Sharpenn ing | 0.87414 | **0.95019** | 0.90326 | **0.93317** | 0.93011 | **0.95518** | 0.91084 | **0.92884** | 0.94194 | **0.95003** |
| Làm mờ (Blur) | 0.49682 | **0.8814** | 0.61922 | **0.88519** | 0.64215 | **0.89293** | 0.60383 | **0.90287** | 0.68032 | **0.90587** |
| Nén JPEG | 0.71298 | **0.78889** | 0.69397 | **0.84741** | 0.74213 | **0.86872** | 0.72753 | **0.841** | 0.74494 | **0.84613** |



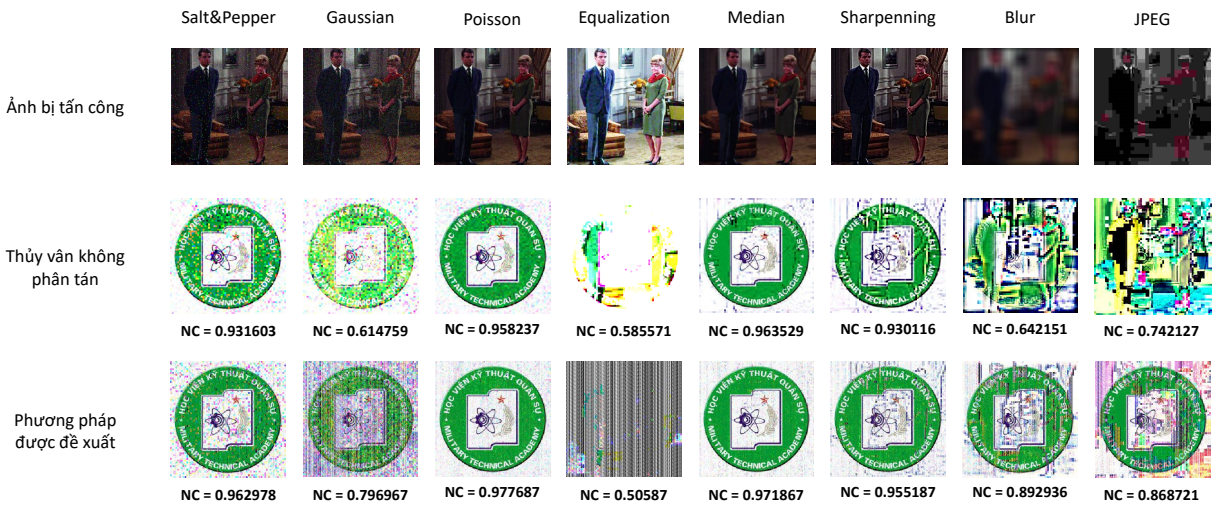

Hình 11: So sánh, đánh giá giữa thủy vân không phân tán và thủy vân phân tán được đề xuất trên ảnh chứa Lena

*1) Tính không thể nhận biết được:* Chúng tôi đã đánh giá tính chất này của ảnh sau khi được nhúng thủy vân bằng thuật toán kết hợp mật mã trực quan và DWT bằng cách đo PSNR giữa ảnh gốc và ảnh đã được nhúng thủy vân cũng như tiến hành đo giá trị NC giữa thủy vân gốc và thủy vân sau khi trích xuất.

Kết quả của quá trình nhúng và trích xuất thủy vân của ảnh Lena được thể hiện trong Hình 8. Kết quả sau khi nhúng ảnh phân tán logo Hình 8(b)

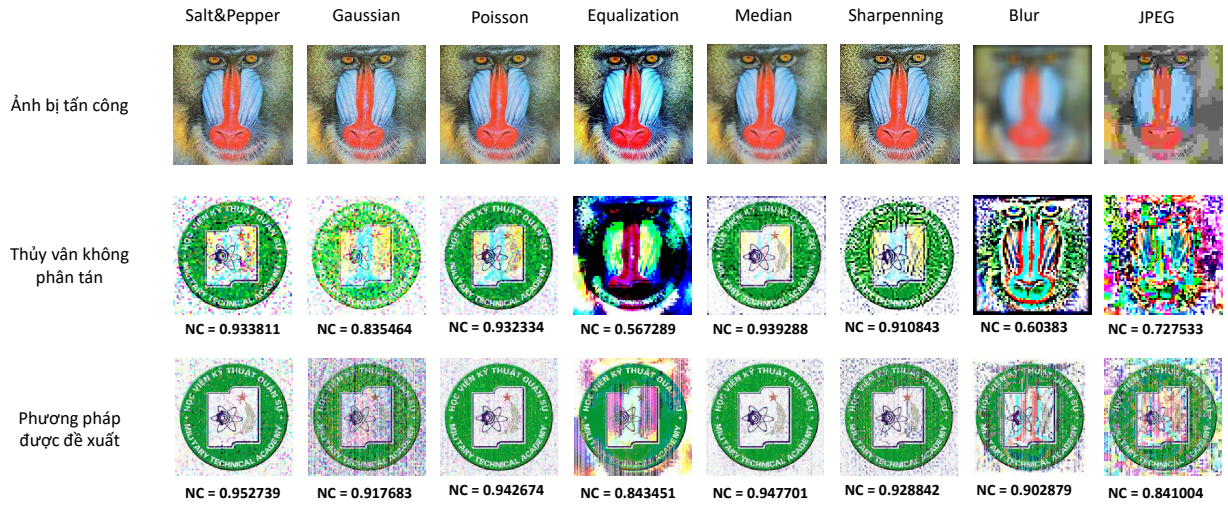



Hình 12: So sánh, đánh giá giữa thủy vân không phân tán và thủy vân phân tán được đề xuất trên ảnh chứa Pepper

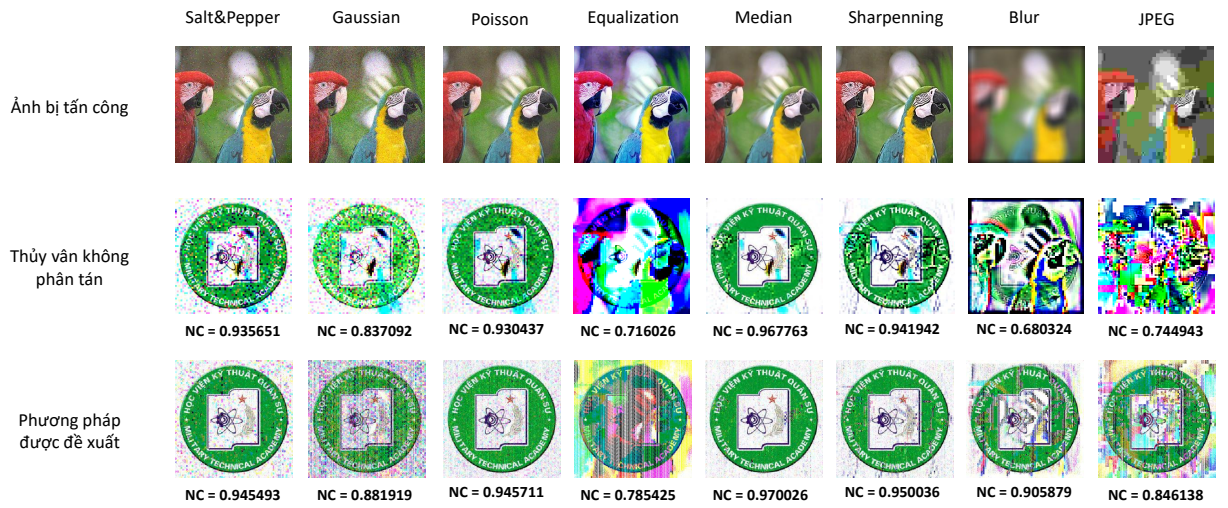



Hình 13: So sánh, đánh giá giữa thủy vân không phân tán và thủy vân phân tán được đề xuất trên ảnh chứa Couple

vào ảnh gốc ở Hình 8(a), ta thu được ảnh nhúng thông tin Hình 8(c) với giá trị PSNR = 34.7672dB. Hình ảnh logo sau khi trích rút được thể hiện trong Hình 8(d).




Hình 14: So sánh, đánh giá giữa thủy vân không phân tán và thủy vân phân tán được đề xuất trên ảnh chứa Mandrill




Hình 15: So sánh, đánh giá giữa thủy vân không phân tán và thủy vân phân tán được đề xuất trên ảnh chứa Parrots

Chúng tôi cũng thử nghiệm trên một số ảnh chứa thủy vân khác và thu được kết quả như Bảng I. Từ kết quả này cho thấy giải pháp thuỷ vân đề xuất tương đối hiệu quả với 5 ảnh màu mà

chúng tôi đã lựa chọn để thực nghiệm.

*2) Tính bền vững:* Hình 9 cho thấy kết quả thử nghiệm trích xuất thủy vân từ dải LL2 của ảnh chứa Lena sau khi chịu các cuộc tấn công khác nhau. Ta thấy được rõ ràng, với những tấn công ảnh hưởng nhiều đến chất lượng ảnh chứa thuỷ vân, thông tin bản quyền của ảnh vẫn có thể đảm bảo được xác thực rõ nét với hình ảnh của logo được nhúng trong ảnh thuỷ vân.

Bảng II thể hiện giá trị NC giữa thủy vân gốc và thủy vân được trích xuất từ băng con LL2 của ảnh Lena chứa thông tin bản quyền sau khi chịu sự ảnh hưởng của các loại tấn công khác nhau.

### *E. Kết quả thí nghiệm và so sánh*

Tại phần này, chúng tôi tiếp tục thử nghiệm trên ảnh Lena với thủy vân không phân tán và so sánh với kết quả thử nghiệm ở phần trước để đánh giá hiệu quả của thuật toán.

Hình 10 so sánh kết quả nhúng và trích thủy vân khi sử dụng thủy vân không phân tán và thủy vân phân tán. Từ kết quả này ta thấy được nếu nhúng logo không phân tán thì dung lượng logo nhúng vào trong ảnh gốc sẽ rất lớn, dẫn đến chất lượng ảnh sau khi nhúng thông tin sẽ bị ảnh hưởng rất nhiều. Điều này chỉ ra rằng phương án đề xuất của chúng tôi sẽ đạt ưu điểm hơn so với phương án nhúng thuỷ vân không phân tán.

Thử nghiệm thuật toán khi sử dụng thủy vân không phân tán trong điều kiện ảnh được nhúng thủy vân chịu ảnh hưởng của một số loại tấn công. Kết quả được thể hiện trong Bảng III. Từ kết quả thử nghiệm của Bảng III, ta thấy được phương án đề xuất có ưu điểm tốt hơn so với phương án chỉ sử dụng thuỷ vân trên miền tần số DWT.

So sánh các giá trị NC giữa 2 phương pháp thủy vân được lấy từ Bảng III và kết quả trực quan trên các Hình 11; 12; 13; 14 và 15 cho thấy khi ảnh thuỷ vân không phân tán bị tấn công dưới những phép biến đổi ảnh mạnh, tính bền vững của logo không được đảm bảo như ảnh thuỷ vân phân tán. Đặc biệt, một số tấn công như equalization, blur, nén JPEG đã làm biến đổi hoàn toàn thông tin logo đã được nhúng vào trong ảnh gốc ban đầu.

## V. KẾT LUẬN

Bài báo của chúng tôi đã đề xuất một giải pháp bảo vệ bản quyền ảnh số dựa trên phương pháp kết hợp thuỷ vân số với hệ mật mã trực quan để tạo ra được một phương pháp bền vững và hiệu quả hơn trong ứng dụng bảo vệ bản quyền sản phẩm số.

Từ các kết quả thu được qua các thử nghiệm khác nhau với thuật toán khi sử dụng cả thủy vân phân tán và không phân tán. Chúng tôi nhận thấy rằng, khi sử dụng thủy vân không phân tán, chất lượng ảnh sau khi nhúng thủy vân kém hơn so với sử dụng thủy vân phân tán. Tuy nhiên, chất lượng thủy vân sau khi trích xuất của thủy vân không phân tán lại tốt hơn.

Đối với các thử nghiệm trong điều kiện có ảnh hưởng của các cuộc tấn công cho thấy rằng: việc sử dụng thủy vân phân tán sẽ đảm bảo tính bền vững của thủy vân hơn so với sử dụng thủy vân không phân tán.

Như vậy, trong bài báo này chúng tôi đã chỉ ra rằng: với việc áp dụng kỹ thuật mật mã trực quan để phân tán thủy vân, đồng thời kết hợp thuật toán thủy vân dựa trên phép biến đổi sóng con rời rạc DWT, đã góp phần nâng cao tính không thể nhận biết được cũng như tính bền vững của thủy vân trước các phép tấn công thông thường.

## ACKNOWLEDGEMENT

Nghiên cứu này được tài trợ bởi Quỹ Phát triển khoa học và công nghệ Quốc gia (NAFOSTED) trong đề tài mã số 102.01-2019.12

## TÀI LIỆU THAM KHẢO

[1] Hsu C. T., Wu J. L., "Hidden digital watermarks in images," IEEE Transactions on image processing, 8(1), pp.58-68, 1999.

[2] Das C., Panigrahi S., Sharma V. K., Mahapatra, K. K., "A novel blind robust image watermarking in DCT domain using inter-block coefficient correlation," AEU International Journal of Electronics and Communications, 68(3), pp. 244-253, 2014.

[3] Zear A., Singh A. K., Kumar P., "A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine," Multimedia Tools and Applications, pp. 1–20, 2016.

[4] Singh A. K., Kumar B., Singh S. K., Ghrera S. P., Mohan, A., "Multiple watermarking technique for securing online social network contents using Back Propagation Neural Network," Future Generation Computer Systems, 2016.

[5] Barni M., Bartolini F., Piva, A., "Improved wavelet-based watermarking through pixel-wise masking," IEEE transactions on image processing, 10(5), pp.783–791, 2001.

[6] Singh A. K., Kumar B., Dave M., Mohan A., "Robust and imperceptible dual watermarking for telemedicine applications," Wireless Personal Communications, 80(4), pp. 1415–1433, 2015.

[7] Singh A. K., Dave M., Mohan A.,“ Robust and secure multiple watermarking in wavelet domain,” Journal of medical imaging and health informatics, 5(2), pp. 406–414, 2015.
[8] Singh AK, Dave M, Mohan A, “Hybrid technique for robust and imperceptible multiple watermarking using medical images,” Multimed Tools Appl:121, 2015.
[9] Urvoy M., Goudia D., Autrusseau F., “Perceptual DFT watermarking with improved detection and robustness to geometrical distortions,” IEEE Transactions on Information Forensics and Security, 9(7), pp. 1108–1119, 2014.
[10] Cedillo-Hernandez M., Garcia-Ugalde F., Nakano-Miyatake M., Perez-Meana H., “Robust digital image watermarking using interest points and DFT domain,” In: 35th IEEE International Conference on Telecommunications and Signal Processing (TSP), pp. 715–719, 2014.
[11] T. M. Thanh, K. Tanaka, “The novel and robust watermarking method based on $q$-logarithm frequency domain,” Multimedia Tools and Applications, volume 75, pp. 11097–11125, 2016.
[12] T. M. Thanh, K. Tanaka,“A proposal of novel $q$-DWT for blind and robust image watermarking,” Proceeding of IEEE 25th International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC), Washington D.C., pp. 2066–2070, 2014.
[13] T. M. Thanh, P. T. Hiep, T. M. Tam, “A New Spatial q-log Domain for Image Watermarking,” IJIIP: International Journal of Intelligent Information Processing, Vol. 5, No. 1, pp.12–20, ISSN 2093-1964, 2014.
[14] T. M. Thanh, K. Tanaka, “An image zero-watermarking algorithm based on the encryption of visual map feature with watermark information,” International Journal of Multimedia Tools and Applications (MTAP), ISSN: pp. 1573–7721, 2016.
[15] M. Naor and A. Shamir, “Visual Cryptography,” Advances in Cryptology (EUROCRYPTO 94), (Lecture Notes in Computer Science), vol. 950, A. De Santis, Ed. Berlin, Germany: Springer-Verlag, pp. 1-12, 1995.
[16] A. Shamir, “How to share a secret?” Comm ACM, 22(11):612-613, 1979.
[17] G. Blakley, “Safeguarding cryptographic keys,” Proc. of AFIPS National Computer Conference, 1979.
[18] C. Asmuth and J. Bloom, “A modular approach to key safeguarding,” IEEE transaction on Information Theory, 29(2), pp. 208–210, 1983.
[19] Shyamalendu Kandar and Bibhas Chandra Dhara, “k-n Secret Sharing Visual Cryptography Scheme on Color Image using Random Sequence,” International Journal of Computer Applications (0975 – 8887) Volume 25– No.11, July 2011.
[20] S. Kumar and R. K. Sharma, “Threshold visual secret sharing based on Boolean operations,” Security and Communication Networks, 2013. DOI:10.1002/sec.769.
[21] Ersin Elbasi and Ahmet M. Eskicioglu, “Naïve Bayes Classifier Based Watermark Detection in Wavelet Transform,” Multimedia Content Representation, Classification and Security. MRCS, Lecture Notes in Computer Science, vol 4105, 2006.
[22] Song Huang and Wei Zang, “Blind Watermarking Scheme Based on Neural Network,” The 7th World Congress on Intelligent Control and Automation, Chongqing, pp. 5985–5989, 2008.
[23] Ngô Nhật Nguyên và Lê Nhật Thắng, “Xây dựng ứng dụng giấu tin trong ảnh,” Đề tài nghiên cứu khoa học, Đại học Lạc Hồng, 2012.
[24] Trần Thị Tú Uyên, “Hệ thống thủy vân số và ứng dụng thủy vân số trong bảo vệ bản quyền ảnh số,” Luận văn Thạc sỹ Công nghệ thông tin, Đại học Công nghệ, 2018.

## A PROPOSAL OF IMAGE COPYRIGHT PROTECTION TECHNIQUE BASED ON THE COMBINATION OF WATERMARKING WITH VISUAL SECRET SHARING

***Tóm tắt*—This paper proposes a solution for digital image copyright protection technique using the combination of watermarking and visual encryption technique. In our solution, the copyright information (copyright logo) is distributed into $n$ shares using $k - out - of - n$ distributed algorithm, also called $(k, n)$ visual secret sharing method. One of the shares is randomly selected to embed into the original image to prove the user's copyright. The remaining $n - 1$ shares is used to register with Vietnamese Copyright Office. When claiming the copyright belongs to the user, the verifier only needs to extract the watermark information from the watermarked image, then decodes with any registered $k - 1$ shares from $n - 1$ shares for restoring copyright information. Experimental results of the proposed method compared with the method using only digital watermark show that our method has more practical effectiveness in the application of digital product copyright protection.**

***Từ khóa*—Digital watermarking, visual secret sharing - VSS, Copyright Protection, Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), Copyright authority.**

**Giang Ngọc Dân** Hiện đang theo học kỹ sư Công nghệ mạng tại trường Đại học Lê Quý Đôn.

Lĩnh vực nghiên cứu thuộc lĩnh vực thủy vân số.

**Tạ Minh Thanh** nhận bằng kỹ sư CNTT và Thạc sĩ Khoa học Máy tính của Học viện Phòng vệ Nhật Bản, vào năm 2005 và 2008. Ông Thanh là giảng viên của trường Đại học Lê Quý Đôn từ năm 2005. Năm 2015, ông nhận bằng Tiến sĩ Khoa học Máy tính của Học viện Công nghệ Tokyo, Nhật Bản. Ông đã được công nhận chức danh Phó giáo sư của Hội đồng Giáo sư nhà nước vào năm 2019. Ông cũng là thành viên của Hiệp hội IPSJ Nhật Bản và Hiệp hội IEEE.

Lĩnh vực nghiên cứu của ông thuộc lĩnh vực thủy vân số, công nghệ mạng, bảo mật thông tin và thị giác máy.