

KỸ THUẬT THỦY VÂN ẢNH SỐ SỬ DỤNG ROI VÀ EXTRACTION VOTING TRÊN MIỀN TẦN SỐ

Lê Danh Tài*, Tống Minh Đức* Tạ Minh Thanh†*

* Học Viện Kỹ Thuật Quân Sự, 236 Hoàng Quốc Việt, Bắc Từ Liêm, Hà Nội

Tóm tắt—Trong các thuật toán thủy vân ảnh số, mục tiêu quan trọng đó là tăng cường độ bền vững của thông tin mật và không giảm chất lượng ảnh thủy vân. Cụ thể, ảnh khi được nhúng thông tin mật không thể bị phát hiện sự thay đổi cũng như khó trích rút thông tin đã nhúng bằng một số phương pháp thông thường. Độ bền vững thể hiện khi bị tấn công thủy vân, thuật toán đề xuất có khả năng trích rút thông tin mật có độ chính xác cao. Vì vậy, trong giai đoạn nhúng, chúng tôi sử dụng giá trị ngưỡng T để tìm ra vùng dữ liệu ảnh ROI thích hợp và lưu trữ thông tin ROI trong ma trận Mat . Tiếp theo, sử dụng biến đổi DCT cho vùng ROI đã chọn và kỹ thuật QIM để nhúng thông tin mật là chuỗi các bit 0 và 1. Các bit được nhúng một hoặc nhiều lần trên một hoặc nhiều vị trí khác nhau. Ở giai đoạn trích rút, sử dụng khóa K là ma trận Mat để xác định các vị trí chứa thông tin mật đã nhúng. Sau đó, thực hiện trích rút thông tin mật dựa trên kỹ thuật Extraction Voting. Thông tin mật được voting dựa trên tỉ lệ trích rút các bit 0 và 1 để đưa ra kết quả chính xác nhất. Việc sử dụng ROI và Extraction Voting giúp cải tiến độ chính xác thông tin trích rút khi chống lại các phép tấn công thủy vân và không giảm chất lượng ảnh số sau khi nhúng thông tin.

Từ khóa—Thủy vân ảnh kỹ thuật số, Vùng quan tâm (ROI), Trích rút bỏ phiếu, Điều chế chỉ số lượng tử (QIM)

I. GIỚI THIỆU

A. Tổng quan

Ngày nay, các sản phẩm multimedia như video, âm thanh, hình ảnh, văn bản được sản xuất và truyền đi

một cách nhanh chóng, phục vụ mục đích giải trí, thương mại. Chúng dễ dàng được sao chép, phát tán. Nhiều người không được cấp quyền cũng dễ dàng truy cập và kiếm lợi nhuận từ những sản phẩm không phải của mình. Hành vi sao chép, chia sẻ, sửa đổi khi không có sự cho phép chủ sở hữu hợp pháp là vi phạm bản quyền sản phẩm số. Hiện tượng này thường xuyên xảy ra trên mạng internet. Vì vậy, nhà sản xuất hoặc chủ sở hữu hợp pháp các sản phẩm multimedia có nhu cầu cao đối với việc bảo vệ bản quyền sản phẩm của họ.

Thủy vân số - Digital watermarking [1] là một giải pháp kỹ thuật đáp ứng nhu cầu bảo vệ bản quyền các sản phẩm số. Các thông tin mật (thông tin bản quyền, logo, thông tin tác giả, chữ ký số, ...) được mã hóa và nhúng vào dữ liệu đa phương tiện mà không làm ảnh hưởng đến chất lượng để làm căn cứ khi xảy ra tranh chấp hoặc xử lý vi phạm bản quyền. Khi xảy ra tranh chấp, thông tin mật sẽ được trích rút dựa vào khóa bí mật. Từ đó, chứng minh quyền sở hữu hợp pháp đối với sản phẩm số.

Thủy vân ảnh số [1] [2] là một trong các kỹ thuật thủy vân phổ biến, được nghiên cứu và ứng dụng rộng rãi trong lĩnh vực bảo vệ bản quyền ảnh số. Các nhà nghiên cứu đã phát triển nhiều lược đồ thủy vân trên miền không gian và miền tần số. Đặc biệt, kỹ thuật thủy vân ảnh số phát triển mạnh trên các miền tần số sử dụng các biến đổi DCT, SVD, DWT [2], [5]–[8], [11], [18], [19] hoặc các miền tần số kết hợp [9], [12]. Họ khai thác các đặc tính của mỗi miền dữ liệu để tăng cường tính bền vững [9], tính ẩn, cải thiện tốc độ tính toán cũng như khả năng ẩn giấu thông tin mật trong các lược đồ thủy vân.

Trong nhiều lược đồ thủy vân, các tác giả thường nhúng thông tin lên toàn bộ các vùng của ảnh mang thông qua các phép biến đổi [5], [7], [9], [12], [15]. Kỹ thuật này đảm bảo nhúng được lượng thông tin

Tác giả liên hệ: Lê Danh Tài,
Email: ledanhtai@lqdtu.edu.vn.

Đến tòa soạn: 25/7/2021, chỉnh sửa: 31/8/2021,
chấp nhận đăng: 26/9/2021.

† Corresponding author

lớn. Tuy nhiên, việc tác động lên toàn bộ các vùng dữ liệu đã phần nào làm giảm đi chất lượng của ảnh mang. Mặt khác, các thông tin ẩn giấu thường có kích thước nhỏ hơn nhiều lần so với ảnh mang. Vì vậy, nên chẳng lựa chọn các vùng phù hợp ở trên ảnh để nhúng thông tin mật, từ đó tránh làm giảm chất lượng của ảnh mang mà vẫn đảm bảo sử dụng để chứng minh bản quyền khi cần thiết.

Qasim và cộng sự [3] đã áp dụng lược đồ thủy văn cho các ảnh chụp MR não trong y tế. Sử dụng ROI (Region Of Interest) để xác định vùng nhúng dữ liệu và vùng không nhúng dữ liệu. Vùng sử dụng nhúng dữ liệu là vùng ROI (nền) có độ mượt cao hơn (có độ chênh lệch giá trị màu giữa các điểm ảnh thấp) và vùng không quan tâm tới RONI (phần dữ liệu quan trọng của ảnh hoặc không được phép tác động vào). Ngưỡng T được dùng để xác định ROI được chọn bằng cách thử nghiệm trên một tập nhiều ảnh đa dạng và ước lượng giá trị thích hợp. Lược đồ thủy văn được các tác giả trình bày là lược đồ thủy văn thuận nghịch, nhằm phát hiện ra sự thay đổi của các bức ảnh y tế chụp não bộ của bệnh nhân.

Jeya và cộng sự [4] cũng đề xuất lược đồ thủy văn trên vùng dữ liệu RONI (Region-Of-None-Interest) áp dụng trên ảnh CT của bệnh viêm phổi trong y tế. Việc xác định RONI và nhúng thông tin mật lên đó để tránh làm thay đổi thông tin quan trọng của ảnh.

Keshavarzian và cộng sự [18] đã đề xuất lược đồ thủy văn trên vùng dữ liệu ROI kết hợp biến đổi DWT đảm bảo tính khó nhận biết, tính bền vững và tính bảo mật. Trong đó, các tác giả sử dụng vùng ROI của ảnh mang làm thông tin mật và được nhúng vào các băng con tần số thấp trong ảnh mang khi áp dụng biến đổi DWT. Để tăng tính bảo mật, các tác giả sử dụng biến đổi Arnold cho băng con LL của ROI và khối ảnh mang ban đầu. Tuy nhiên, việc là này tăng thêm độ phức tạp của thuật toán.

Ngoài ra, các tác giả khác đã đề xuất các lược đồ thủy văn trên miền tần số và các miền tần số kết hợp áp dụng cho mục đích bảo vệ bản quyền. Mỗi lược đồ đều khai thác tối đa các đặc tính quan trọng của các miền tần số, để tăng cường tính bền vững của lược đồ thủy văn, giúp ảnh thủy văn chống lại các tấn công biến đổi hình học, tấn công nén, tấn công gây nhiễu ... Các miền tần số thường được sử dụng nhiều như DCT, SVD, DWT, DFT, ...

Bên cạnh đó, để tăng cường tính bảo mật của thông tin giấu, các tác giả thường mã hóa [6], [8], [12], [15], [18] thông tin mật trước khi nhúng. Để đảm bảo khi bị tấn công dò thủy văn cũng khó có thể giải mã

được chính xác thông tin mật. Trong các thí nghiệm, kỹ thuật xáo trộn Arnold Transform được sử dụng phổ biến hơn cả [8], [12], [15], [18], [19].

Như vậy, trong các lược đồ thủy văn ảnh số, không phải lúc nào thông tin mật cũng được nhúng trên toàn ảnh. Bên cạnh đó, kích thước thông tin mật thường nhỏ hơn nhiều so với kích thước ảnh mang. Vì vậy, phân tích để xác định được vùng dữ liệu nào được sử dụng để xử lý nhúng thủy văn sẽ là một bước quan trọng để tăng cường chất lượng ảnh sau khi nhúng thủy văn, nhưng vẫn đảm bảo được tính bền vững, tính bảo mật của thông tin mật được giấu. Do đó, xác định vùng quan tâm ROI là bước cần thiết trước khi thực hiện các kỹ thuật nhúng thủy văn.

Trong kỹ thuật xử lý ảnh hoặc trong lĩnh vực thị giác máy tính, ROI có thể là bất cứ hình dạng nào, có thể hình vuông, chữ nhật, tròn, hoặc nhiều vùng nhỏ trên ảnh hoặc thậm chí là các pixel. Với các vùng ROI lớn, nếu sử dụng để nhúng thông tin thì sẽ đảm bảo các vùng khác không bị tác động, làm cho chất lượng ảnh ở đó không bị thay đổi, còn các vùng bị tác động chỉ thay đổi ở mức thấp nhất. Do đó, chất lượng ảnh tổng hợp sau khi nhúng thủy văn sẽ tốt hơn. Nhưng lại đối diện với nguy cơ mất thông tin ẩn giấu nhiều hơn khi bị tấn công thủy văn bởi các kỹ thuật như cắt ảnh, ghép ảnh. Do đó, việc xác định ROI là bước quan trọng. Vì vậy, ở trong thí nghiệm này, ảnh mang sẽ được chia thành các khối có kích thước 8x8 không trùng lặp. Trên mỗi khối sẽ tính giá trị phương sai [16] theo công thức (1) để xác định xem khối có thích hợp để nhúng thông tin hay không. Đồng thời lưu lại thông tin của các khối được chọn để làm chìa khóa cho quá trình trích rút thông tin. Bên cạnh đó, để tăng cường độ chính xác, thông tin sẽ được nhúng trên cả 3 kênh màu của ảnh đầu vào. Do đó, khi trích rút, ngoài việc dùng các khóa như trên, còn kết hợp thêm kỹ thuật bỏ phiếu (voting) để tăng cường độ chính xác.

Giá trị phương sai của khối các điểm ảnh có kích thước $N \times M$ được tính theo công thức sau [16]:

$$\delta^2 = \frac{1}{MN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (F_{i,j} - \bar{F})^2 \quad (1)$$

Trong đó, δ là giá trị phương sai; $F_{i,j}$ là giá trị điểm ảnh tại tọa độ i, j ; $\bar{F}$ là giá trị trung cộng của các điểm ảnh trong khối.

B. Các mục của bài báo

Phần còn lại của bài báo được tổ chức như sau. Đề xuất lược đồ thủy vân trong mục II. Thí nghiệm và kết quả của lược đồ thủy vân đề xuất được trình bày trong mục III. Mục IV là kết luận và đề xuất hướng nghiên cứu tiếp theo.

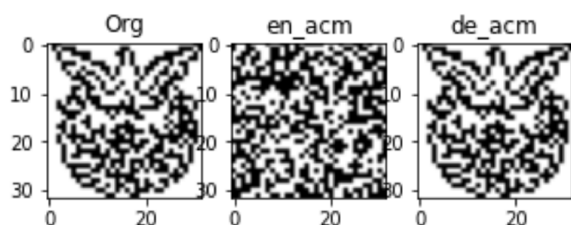
II. ĐỀ XUẤT LƯỢC ĐỒ THỦY VÂN

A. Biến đổi Arnold logo

Trong lược đồ thủy vân, để tăng cường bảo mật, thông tin mật là logo bản quyền được mã hóa sử dụng kỹ thuật xáo trộn Arnold [8], [12], [15], [18]. Xét ảnh đầu vào có kích thước $N \times N$ được mã hóa bằng cách xáo trộn các điểm ảnh theo phương trình sau [15], [18]:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \mod N \quad (2)$$

Trong đó, x, y tương ứng là tọa độ của ảnh gốc; x', y' tương ứng là tọa độ của điểm ảnh bị xáo trộn. Biến đổi Arnold thực hiện hoán đổi vị trí của các pixel trong ảnh nhiều lần. Với $N=32$ thì sau 24 lần lặp, hình ảnh xáo trộn sẽ bằng với hình ảnh ban đầu. Do đó, để mã hóa logo thông tin mật bằng biến đổi Arnold, khóa “key wm” là một số nguyên sẽ được truyền vào và thực hiện xáo trộn “key wm” lần.



Hình 1: Biến đổi Arnold với khóa “key wm”
Từ trái sang phải: Logo gốc, Logo mã hóa, Logo giải mã

B. Xác định vùng dữ liệu nhúng thông tin ROI

Vùng quan tâm ROI là vùng dữ liệu được sử dụng cho mục đích nhúng thông tin mật mà không làm giảm chất lượng ảnh mang. Ở đây, ảnh mang được chia thành các khối 8×8 riêng biệt. Trên mỗi khối, tính giá trị phương sai theo công thức (1). Để đánh giá khối có phù hợp để nhúng thông tin không, thực hiện so sánh giá trị phương sai với ngưỡng T . Các khối thỏa mãn sẽ được lưu lại thông tin vào ma trận Mat để làm khóa cho quá trình trích rút thông tin

mật và được gán giá trị là 1. Ngược lại, các khối không được chọn để nhúng thông tin được gán giá trị là 0. Thông tin vị trí các khối được lưu lại dưới dạng ma trận nhị phân Mat . Ma trận Mat được mã hóa (AES) và gửi cho cơ quan quản lý, chứng thực bản quyền CA (Certificate Authority). Khi có tranh chấp xảy ra, CA sẽ cung cấp “bộ khóa” trong đó có ma trận Mat chứa thông tin vị trí nhúng, để trích rút thông tin bản quyền.

Ngưỡng T là giá trị để đánh giá xem khối có phù hợp để nhúng thông tin mật. Giá trị của T được xác định thông qua quá trình thực nghiệm trên tập hợp gồm nhiều ảnh khác nhau và có thể điều chỉnh phù hợp với từng tập dữ liệu. Tuy nhiên T phải đảm bảo là lớn hơn giá trị phương sai nhỏ nhất và nhỏ hơn giá trị phương sai lớn nhất của ảnh. Việc xác định giá trị T cũng cần phải căn cứ vào tương quan kích thước giữa logo bản quyền (thông tin mật) và kích thước của ảnh mang.



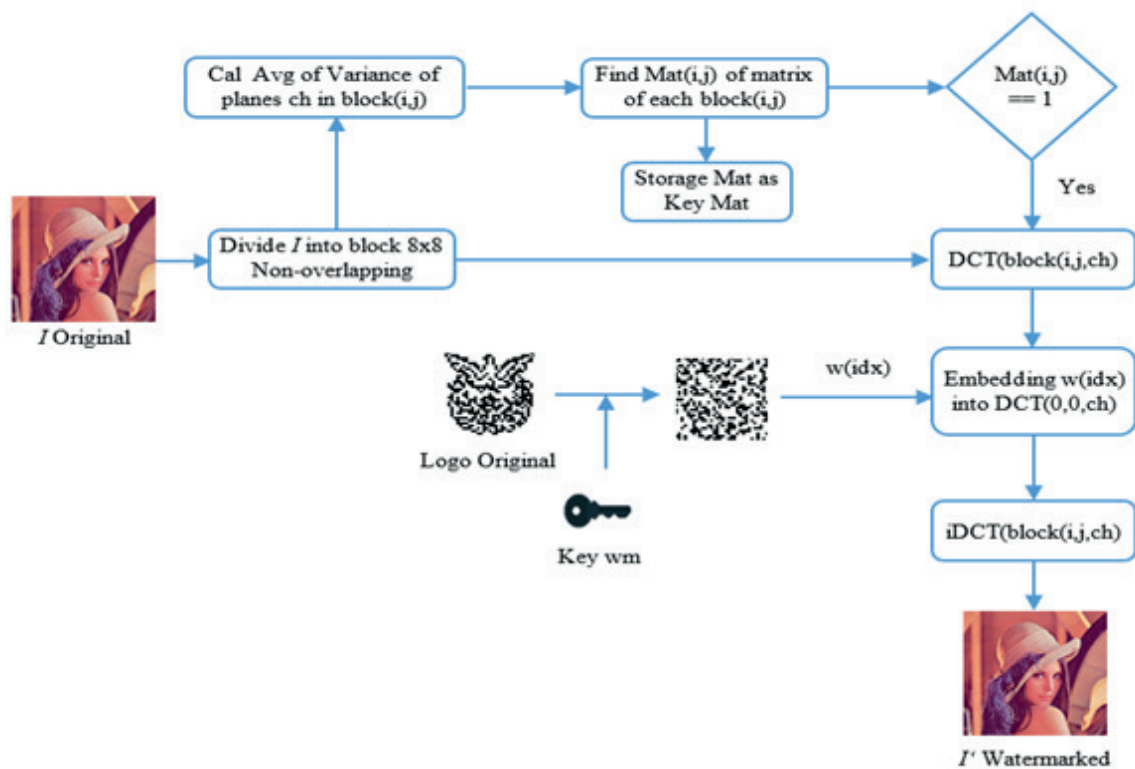
Hình 2: Ma trận các vị trí ROI được chọn

C. Tiến trình nhúng thủy vân

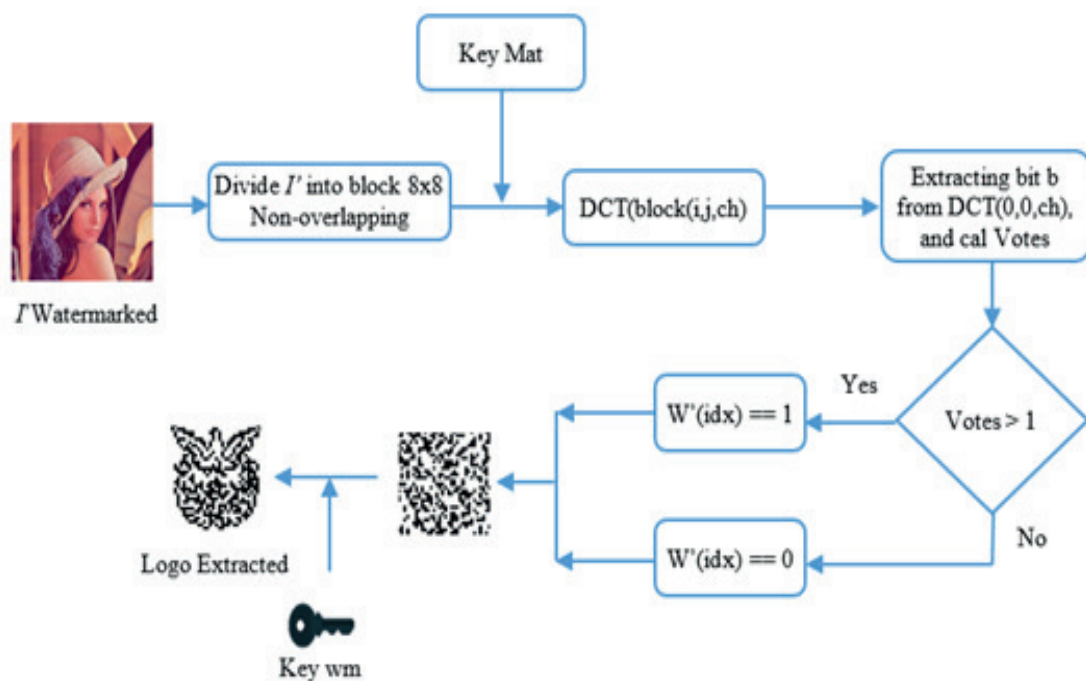
Trong quá trình nhúng thủy vân, sử dụng biến đổi DCT [6], [7], [9], [11] và kỹ thuật QIM [7], [14] để nhúng thông tin. Khối được chọn sẽ được biến đổi DCT 2 chiều, chọn phần tử $DCT[0,0]$ chứa nhiều năng lượng ảnh nhất, để tác động theo kỹ thuật QIM với trọng số nhúng $q = 0.01$. Phương trình nhúng cụ thể:

$$E'(i, j) = \begin{cases} \lfloor \frac{E(i, j)}{q} \rfloor q + \text{sgn}(\frac{3q}{4}) & \text{với } w(k) = 1 \\ \lfloor \frac{E(i, j)}{q} \rfloor q + \text{sgn}(\frac{q}{4}) & \text{với } w(k) = 0 \end{cases} \quad (3)$$

Trong đó, $E(i, j)$ là giá trị DCT tại vị trí $[0, 0, ch]$; $E'(i, j)$ là giá trị DCT tại vị trí $[0, 0, ch]$ nhận được sau khi nhúng thông tin; $w(k)$ là giá trị bit nhị phân tại vị trí thứ k của chuỗi thông tin mật.



Hình 3: Lược đồ nhúng thủy văn sử dụng ROI



Hình 4: Lược đồ trích rút thủy văn sử dụng ROI và Voting

Các bước thực hiện của quá trình nhúng thủy vân như sau:

Bước 1: Chia ảnh mang I thành các block 8×8 không trùng lặp

Bước 2: Tính giá trị trung bình avg phương sai của 3 plane trên mỗi block

Bước 3: Tính ma trận Mat :

Nếu $avg \geq T$ & $\text{count}(Mat[i, j] == 1) \leq wm_{len}$ thì:

$$Mat[i, j] = 1$$

Ngược lại:

$$Mat[i, j] = 0$$

Bước 4: Sử dụng Arnold Transform để mã hóa logo w với key wm

Bước 5: Duyệt ma trận Mat , nếu $Mat[i, j] == 1$ thì thực hiện:

Trên mỗi plane ch :

- Biến đổi DCT $block[i, j, ch]$

- Sử dụng phương trình (3) để nhúng bit $w(idx)$ vào $DCT[0, 0, ch]$

- Biến đổi iDCT $block[i, j, ch]$

Bước 6: Khôi phục I ta thu được ảnh I' đã được nhúng thông tin mật

Sau khi thực hiện nhúng thủy vân, ảnh số được phân phối tới người dùng hợp pháp. Các giá trị “key wm ”, ma trận thông tin ROI Mat , trọng số nhúng q được lưu trữ thành bộ khóa $K(key\ wm, Mat, q)$. Bộ khóa K được mã hóa (AES) và gửi lên cơ quan quản lý bản quyền CA (Certificate Authority). Khi xảy ra tranh chấp, CA sẽ cung cấp bộ khóa và tiến hành trích rút thông tin để chứng minh quyền sở hữu hợp pháp.

D. Tiến trình trích rút thủy vân sử dụng Voting

Khi xảy ra tranh chấp, CA sẽ giải mã và cung cấp bộ khóa $K(key\ wm, Mat, q)$. Ma trận Mat được sử dụng để xác định các vị trí đã giấu thông tin mật; trọng số q dùng để trích rút thông tin mật theo phương trình (4); khóa “key wm ” được dùng để giải mã thông tin mật thu được.

Để trích rút thông tin, sử dụng phương trình (4) như sau:

$$w'(idx) = \begin{cases} 1 & \text{Nếu } E'(i, j) - \lfloor \frac{E'(i, j)}{q} \rfloor q \geq \frac{q}{2} \\ 0 & \text{Nếu } E'(i, j) - \lfloor \frac{E'(i, j)}{q} \rfloor q < \frac{q}{2} \end{cases} \quad (4)$$

Trong đó, $E'(i, j)$ là giá trị DCT tại vị trí $[0, 0, ch]$, q là trọng số nhúng, $w'(idx)$ là giá trị thứ idx được trích rút từ $E'(i, j)$.

Khi thực hiện trích rút thông tin mật b trên từng plane ch , so sánh với các giá trị 0 và 1 để tính toán $Vote$. Sau đó thực hiện voting để tìm ra bit $w'(idx)$ thích hợp nhất. Các bước thực hiện trích rút thủy vân cụ thể:

Bước 1: Chia ảnh mang I' thành các block 8×8 không trùng lặp

Bước 2: Duyệt ma trận Mat , nếu $Mat[i, j] == 1$ thì thực hiện:

Bước 2.1: $Vote = 0$

Bước 2.2: Trên mỗi plane ch :

- Biến đổi DCT $block[i, j, ch]$

- Sử dụng phương trình (4) để tính ra bit b

- Nếu $b == 1$ thì:

$$Vote = Vote + 1$$

Bước 2.3: Nếu $Vote > 1.5$ thì:

$$w'(idx) = 1$$

Ngược lại:

$$w'(idx) = 0$$

Bước 3: Khôi phục w' sử dụng key wm thu được ảnh logo w'

III. THÍ NGHIỆM VÀ KẾT QUẢ

A. Các độ đo sử dụng đánh giá lược đồ thủy vân

Để đánh giá chất lượng của ảnh mang trước và sau thực hiện nhúng thủy vân số, sử dụng tỉ số tín hiệu cực đại trên nhiễu PSNR (Peak Signal to Noise Rate) [7]. Giá trị PSNR thể hiện chất lượng của ảnh bị thay đổi nhiều hay ít khi tác động thủy vân. Khi giá trị PSNR nhỏ, sự thay đổi nhiều nên dễ dàng bị nhận thấy. Ngược lại, giá trị PSNR cao thể hiện khó có thể cảm nhận được sự thay đổi của ảnh sau khi nhúng thông tin. Do đó, giá trị của độ đo PSNR càng cao càng tốt. PSNR được tính bằng công thức (5) dưới đây:

$$PSNR = 10 \times \log_{10} \times \frac{MAX^2}{MSE} \quad (5)$$

Trong đó, MAX là giá trị lớn nhất có thể của pixel trong ảnh. Khi các pixel được biểu diễn bởi 8 bits, thì giá trị của nó là 255. MSE (Mean Squared Error) là sai số bình phương trung bình tính trên toàn ảnh, được tính theo công thức (6):

$$MSE = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [I(i, j) - I'(i, j)]^2 \quad (6)$$

Với M, N lần lượt là kích thước của ảnh. $I(i, j)$ và $I'(i, j)$ tương ứng là giá trị điểm ảnh tại vị trí i, j của ảnh mang ban đầu và ảnh đã nhúng thủy vân.

Để đánh giá độ bền vững của lược đồ thủy vân, thực hiện tính NCC (Normalized Cross Correlation) của thông tin mật được trích rút sau khi bị tấn công thủy vân (biến đổi hình học, thêm nhiễu, nén ảnh, ...) với thông tin mật ban đầu. Giá trị của NCC càng gần giá trị 1.0 thì chứng tỏ độ bền vững của thủy vân càng tốt. Công thức NCC [13] được tính như sau:

$$NCC = \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [w(i, j) - w'(i, j)]^2}{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [w(i, j)]^2} \quad (7)$$

Với $w(i, j)$ và $w'(i, j)$ tương ứng là giá trị điểm ảnh tại vị trí i, j của logo ban đầu và logo được trích rút.

B. Dữ liệu thí nghiệm

Trong thí nghiệm, sử dụng ảnh tập các ảnh màu có kích thước 512x512 trong bộ dữ liệu ảnh **SIDBA** và ảnh **Logo HVKTQS** (có định dạng .png). Logo sử dụng để nhúng vào là ảnh nhị phân có kích thước 32x32 (Hình 5).



Hình 5: Tập hợp ảnh thí nghiệm (Ảnh mang và logo mark)

Tham số ngưỡng T được xác định bằng 0.005 để xác định các khối pixel (có kích thước 8x8) được lựa chọn (ROI) sao cho tổng số các khối được chọn bằng với độ dài bit của logo sẽ nhúng. Tùy thuộc vào độ dài bit của logo, ma trận Mat thể hiện vị trí khối được chọn thì $Mat(i, j) = 1$, các block không được chọn thì $Mat(i, j) = 0$. Ma trận Mat là một trong những khóa quan trọng được hình thành trong quá trình lựa chọn ROI và tham gia vào quá trình nhúng và trích rút thủy vân. Tiếp theo, giá trị của hệ số nhúng $q = 0.01$ dùng để nhúng thông tin theo

phương trình 3 và trích rút thông tin theo phương trình 4. Các giá trị T và q được lựa chọn sau quá trình thử nghiệm với nhiều ảnh đầu vào khác nhau khi cho kết quả tốt hơn cả. Giá trị q được xem là khóa của lược đồ thủy vân khi tham gia vào cả quá trình nhúng và trích rút thông tin mật.

Như vậy, kết hợp “key w_m ”, Mat và q , lược đồ thủy vân đề xuất có một bộ khóa $K(key\ w_m, Mat, q)$. Sau khi nhúng thủy vân, bộ khóa sẽ được mã hóa và gửi về CA. Khi có tranh chấp, CA sẽ dùng bộ khóa K để trích rút thông tin mật đã giấu.

C. Các phép tấn công thủy vân

TT	Viết tắt	Mô tả kỹ thuật tấn công
1	NA	Không tấn công
2	SN01	Nhiều Salt và Pepper với mật độ = 0.01
3	SN001	Nhiều Salt và Pepper với mật độ = 0.001
4	GN01	Nhiều Gaussian theo phân phối chuẩn variance = 0.01
5	GN02	Nhiều Gaussian theo phân phối chuẩn variance = 0.02
6	EW05	Xóa và thay thế bằng nền trắng, ratio = 0.5 (25%)
7	EB05	Xóa và thay thế bằng nền đen, ratio = 0.5 (25%)
8	BA3	Lọc trung bình với kernel = (3,3)
9	MB3	Lọc trung vị với kernel = 3
10	GB3	Lọc Gaussian với kernel = (3,3)
11	JPEG	Tấn công nén JPEG
12	Color	Tấn công color trên 1 plane

Bảng I: Bảng các phép tấn công thủy vân

Trong thí nghiệm, để đánh giá hiệu quả của lược đồ thủy vân đề xuất, một số phép tấn công thủy vân phổ biến đã được sử dụng như tấn công nhiễu, tấn công nén, tấn công cắt xén, tấn công màu, tấn công lọc ảnh Các phép tấn công thủy vân được sử dụng trong thí nghiệm với các thông số cụ thể trong bảng I.

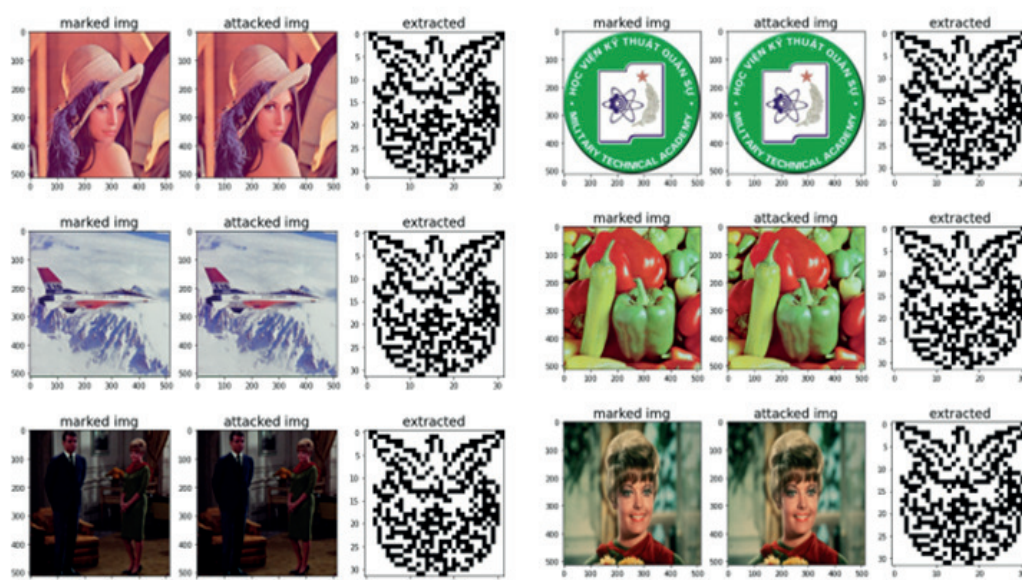
Trong đó, NA là không thực hiện tấn công thủy vân. Các phép tấn công thêm nhiễu Salt & Pepper thực hiện với mật độ 0.01 và 0.001. Tương tự, phép tấn công thêm nhiễu Gaussian theo phân phối chuẩn có variance lần lượt là 0.01 và 0.02. Đối với các phép tấn công bằng các kỹ thuật filter, thực hiện lọc trung bình, lọc Gaussian với cùng kernel bằng (3, 3), lọc trung vị với kernel = 3. Ngoài ra thực hiện tấn công nén Jpeg, thay đổi màu sắc (color change). Các phép

	Lenna	Zelda	Peppers	Airplane	HVKTQS	Couple
PSNR	49.57	49.5	49.57	49.46	49.6	49.58

Bảng II: Bảng kết quả đo PSNR của các ảnh sau khi nhúng thủy vân

	Lenna	Zelda	Peppers	Airplane	HVKTQS	Couple
NA	1.0	1.0	1.0	1.0	1.0	1.0
SN01	0.3863	0.5793	0.5353	0.927	0.6119	0.7099
SN001	0.8841	0.9462	0.959	0.9876	0.9753	0.9565
GN01	0.9856	0.9814	0.971	0.9672	0.9815	0.9917
GN02	0.6677	0.6534	0.6503	0.6396	0.634	0.5916
EW03	0.6596	0.766	0.6796	0.7091	0.9585	0.7652
EB03	0.793	0.8013	0.9167	1.0	1.0	0.6634
BA03	0.963	0.922	0.9238	0.9794	0.8871	0.9735
MB3	0.9057	0.9358	0.9669	0.9836	0.9959	0.9918
GB3	0.9856	0.9589	0.9711	0.9917	0.9298	0.9259
JPEG	1.0	1.0	1.0	1.0	1.0	1.0
Color	1.0	1.0	1.0	1.0	1.0	1.0

Bảng III: Bảng kết quả đo NCC của các logo trích rút được sau khi bị tấn công thủy vân



Hình 6: Kết quả thí nghiệm trên tập ảnh chưa tấn công thủy vân

tấn công làm thay đổi tương đối về chất lượng hình ảnh nhằm phá hủy thông tin mật đã được nhúng.

D. Kết quả thí nghiệm

Hình (6) mô tả kết quả nhúng và trích rút thủy vân của lược đồ đề xuất. Bảng I là số đo PSNR đánh giá tính không thể nhận biết của lược đồ. Các giá trị PSNR đều lớn hơn 49db. Với biện pháp tấn công là NA (không tấn công) logo mật đã nhúng được trích rút một cách chính xác. Theo bảng III, lược đồ áp dụng cho các ảnh mang khác nhau đều cho kết quả trích rút logo mật chính xác cao nhất với $NCC = 1.0$.

Khi thực hiện tấn công bằng các kỹ thuật trong bảng I đối với ảnh Lenna, lược đồ cho kết quả trích rút như hình (7).

Bảng III là kết quả độ đo NCC khi thực hiện các phép tấn công thủy vân trên tập 6 ảnh đầu vào. Đối với các phép tấn công nén JPEG, thay đổi màu (Color change), thí nghiệm cho kết quả trích rút có độ đo NCC rất cao. Các phép tấn công thuộc lớp lọc trung bình, lọc trung vị, lọc Gaussian đều cho kết quả tốt. Tuy nhiên đối với phép tấn công cắt ảnh thì cho kết quả chưa đồng đều. Nguyên nhân thứ nhất là nó phụ thuộc một phần vào cấu trúc của từng ảnh, thứ hai là



Hình 7: Kết quả thực hiện tấn công thủy văn trên ảnh Lenna

nó phụ thuộc vào vị trí cắt, ở đây vị trí cắt là ngẫu nhiên. Nếu vị trí cắt tập trung vào những vùng ảnh ROI đã được chọn thì chất lượng trích rút sẽ bị giảm. Nhưng trong thí nghiệm, kết quả đo NCC vẫn nằm ở vùng có thể nhận dạng ra thông tin. Vì vậy, nếu kết hợp với các kỹ thuật phân tán logo thủy văn khác thì có thể tăng cường độ chính xác của ảnh.

Như vậy, có thể nhận thấy, đối với các phép tấn công trong bảng I thì lược đồ thủy văn đã đề xuất vẫn đảm bảo được tính bền vững, thông tin ẩn giấu được trích rút với độ trích xác cao, đảm bảo nhận dạng và sử dụng cho quá trình giải quyết tranh chấp và bảo vệ bản quyền ảnh số.

IV. KẾT LUẬN

Qua thí nghiệm và các kết quả thu được, việc áp dụng kỹ thuật ROI để xác định vùng dữ liệu ảnh theo lược đồ thủy văn đã đề xuất cho kết quả tương đối tốt. Đối với độ đo PSNR đều $> 49\text{db}$, các ảnh mang nhúng thủy văn đảm bảo tính trong khó nhận biết bằng phương pháp thông thường. Khi tấn công bằng các phép biến đổi ảnh phổ biến, việc trích rút thông tin đã nhúng cho kết quả cao đối với các phép nén, thay đổi màu, lọc trung bình, lọc trung vị, lọc Gaussian. Tuy nhiên, kết quả chưa được tốt khi thực hiện cắt ảnh. Do ở đây khi thực hiện cắt $\frac{1}{4}$ ảnh là tương đối lớn, nhưng vẫn có khả năng trích rút được

một phần quan trọng của thông tin nhúng. Vì vậy, nếu sử dụng các kỹ thuật nhúng phân tán ảnh logo ra nhiều vị trí khác thì có thể cải thiện hiệu quả của kỹ thuật nhúng.

Bên cạnh đó, sử dụng phép biến đổi DCT trên các khối 8x8 điểm ảnh cũng góp phần nâng cao hiệu quả của lược đồ nhúng thủy vân. Tuy nhiên, việc mới chỉ thử nghiệm trên miền DCT cũng chưa thể hiện hết những ưu điểm cũng như hạn chế của lược đồ đề xuất. Vì vậy, trong thời gian tới, cần tiến hành thí nghiệm với nhiều miền không gian khác nhau, đồng thời tìm cách tính toán giá trị ngưỡng T để xác định được vùng ROI đạt hiệu quả nhúng cao hơn. Việc sử dụng kỹ thuật QIM, kết hợp ROI và DCT cùng Voting Extraction hứa hẹn sẽ giúp cải thiện được độ bền vững của thủy vân và chất lượng thông tin trích rút. Việc khoanh vùng các vùng dữ liệu khác nhau để nhúng thông tin và phân tán thông tin cần nhúng ở nhiều nơi khác nhau có thể giúp thủy vân bền vững hơn khi bị tấn công. Do đó, tác giả sẽ tiếp tục nghiên cứu, phát triển trong thời gian tới.

ACKNOWLEDGMENT

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] A. Tefas, N. Nikolaidis, and I. Pitas, "The Essential Guide to Image Processing: Chapter 22 – Image Watermarking: Techniques and Applications". 2st ed. Elsevier, pp. 597–648. 2009.
- [2] Roy S, Pal AK, "An indirect watermark hiding in discrete cosine transform–singular value decomposition domain for copyright protection". R. Soc. Open, sci.4:170326. 2017.
- [3] Qasim, A.F., Aspin, R., Meziane, F. et al, "ROI-based reversible watermarking scheme for ensuring the integrity and authenticity of DICOM MR images". Multimed Tools Appl 78, 16433–16463. 2019.
- [4] Jeya, I. , Suganthi, J., "RONI Based Secured and Authenticated Indexing of Lung CT Images". Computational and Mathematical Methods in Medicine. 2015. 1-9. 10.1155/2015/830453. 2015.
- [5] Tạ Minh Thanh, "Distributed Redundant Image Storages and Reconstruction Algorithm to Contents Verification", The International Conference of National Foundation for Science and Technology Development (NAFOSTED). 2017.
- [6] M. Saidi, H. Hermassi, R. Rhouma, and S. Belghith, "A new adaptive image steganography scheme based on DCT and chaotic map". pp. 13493–13510, 2017. 2017.
- [7] Tạ Minh Thanh, Nguyễn Trung Thanh, "Extended DCT domain for improving the quality of watermarked image", The Seventh International Conference on Knowledge and Systems Engineering (KSE 2015). VIETNAM, 2015.

- [8] D. Asatryan and M. Khalili, "Colour spaces effects on improved discrete wavelet transform-based digital image watermarking using Arnold transform map". IET Signal Process., vol. 7, no. 3, pp. 177–187. 2013.
- [9] A. K. Abdulrahman and S. Ozturk, "A novel hybrid DCT and DWT based robust watermarking algorithm for color images". Multimed. Tools Appl. 2019.
- [10] Katharotiya Anil, Patel Swati, Mahesh Goyani. "Comparative Analysis between DCT and DWT Techniques of Image Compression". Journal of Information Engineering and Applications. 1. 9-17. 2011.
- [11] Lai, C. C, "An improved SVD-based watermarking scheme using human visual characteristics". Optics Communications, 284(4), 938–944, 2011.
- [12] Palak Garg, Lakshita Dodeja, Priyanka and Mayank Dave, "Hybrid Color Image Watermarking Algorithm Based on DSWT-DCT-SVD and Arnold Transform", vol. 526. Springer Singapore. 2019.
- [13] A Ukasha, Majdi Elbireki, and M. Abdullah, "Contour Extraction and Compression from Watermarked Image using Discrete Wavelet Transform and Ramer Method". International Conference on Image Processing and Electronics Engineering (ICIPEE'2013), Penang (Malaysia). 2013.
- [14] M. J. Hwang, J. Lee, M. Lee, and H. G. Kang, "SVD-Based adaptive QIM watermarking on stereo audio signals. IEEE Trans". Multimedia, vol. 20, no. 1, pp. 45–54. 2018.
- [15] M. F. Mohammed, El Bireki, M. F. L. Abdullah, A. A. M. Ukasha, and A. A. Elrowayati, "Digital image watermarking based on joint (DCT-DWT) and Arnold transform". Int. J. Secur. its Appl., vol. 10, no. 5, pp. 107–118. 2016.
- [16] Ariatmanto, D., Ernawan, F, "An improved robust image watermarking by using different embedding strengths". Multimed Tools Appl 79, 12041–12067. 2020.
- [17] Rafael C.Gonzalez, Richard E.Woods. Digital Image Processing. Third Edition.
- [18] Keshavarzian, R., Aghagolzadeh, A. "ROI based robust and secure image watermarking using DWT and Arnold map". AEU - International Journal of Electronics and Communications, 70(3), 278–288. 2016.
- [19] Roy, S., Pal, A. K. A blind DCT based color watermarking algorithm for embedding multiple watermarks. AEU - International Journal of Electronics and Communications, 72, 149–161. 2017

DIGITAL IMAGE WATERMARKING TECHNIQUE USING ROI AND EXTRACTION VOTING ON FREQUENCY DOMAIN

Tóm tắt—In digital image watermarking algorithms, the significant purpose is to improve the robustness of secret information is embedded and not reduce the quality of watermarked images. Specifically, when embedding confidential information into a host image, this host image is difficult to detect had changed and hard to extract embedded information by some conventional methods without using the secret key. Robustness has shown under watermarking attacks, and the proposed algorithms extract confidential

information with high accuracy. So, in the embedding phase, we use the threshold value T to find the appropriate ROI image data region and store the ROI information in the Mat matrix. Next, we use the DCT transform for the chosen ROI region and the QIM technique to embed confidential information in a sequence of bits 0 and 1. The bits are embedded one or more times in one or more different locations. At the extracting stage, use the Mat matrix to determine the locations containing the embedded secret information. Then, perform extracting confidential information based on the Extraction Voting technique. The Secret information is voted based on the extraction rate of bits 0 and 1 to give the most accurate results. Use of ROI and Extraction Voting improves the accuracy of extracted information when resisting watermarking attacks and does not reduce digital image quality after embedding the secret information.

Từ khóa—Digital watermarking, Region of Interest (ROI), Extraction Voting, Quantization Index Modulation (QIM).



Lê Danh Tài tốt nghiệp kỹ sư CNTT và thạc sĩ Khoa học máy tính tại trường Học viện Kỹ thuật quân sự năm 2008 và 2015.

Lĩnh vực nghiên cứu thuộc lĩnh vực thủy văn số, an toàn thông tin, công nghệ mạng.



Tống Minh Đức tốt nghiệp kỹ sư ngành Công nghệ thông tin tại Học viện kỹ thuật quân sự năm 2000. Ông nghiên cứu sinh và nhận bằng tiến sĩ năm 2007 tại trường Đại học Tổng hợp Kỹ thuật điện Xanh Pêtéc-bua – Nga, chuyên ngành Tự động hóa và điều khiển các quy trình công nghệ sản xuất.

Ông là giảng viên của Khoa CNTT trường Học viện kỹ thuật quân sự từ năm 2000. Lĩnh vực nghiên cứu chính là lĩnh vực mật mã, giấu tin, an toàn thông tin.



Tạ Minh Thanh nhận bằng kỹ sư CNTT và Thạc sĩ Khoa học Máy tính vào năm 2005 và 2008. Ông 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 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 văn số, công nghệ mạng, bảo mật thông tin và thị giác máy.