

Phát hiện ảnh giả mạo có các vùng được lấy mẫu tăng dựa trên phép biến đổi hiệu và lọc thông cao DWT

Detection of Upsampled Image Forgery based on Difference Transform and High Pass Filter of DWT

Trần Đăng Hiền, Nguyễn Ngọc Hưng, Phạm Văn Ất

Abstract: In this paper, we present two methods for detecting image forgery that have areas are copied from the various images. The first method is based on difference transform for the 2×2 blocks and the second method is based on high pass filter of DWT (Discrete Wavelet Transform). Compared to some previous methods, proposed methods have lower computational complexity and can detect forgery areas more clearly. Experiments show that the method are more robust against some attacks such as rotation, scaling, add noise, JPEG compression, ...

Keywords: Image forgery, re-sampling detection, DWT discrete wavelet transform.

I. GIỚI THIỆU CHUNG

Ngày nay, ảnh số là phương tiện truyền thông được sử dụng rộng rãi, đóng vai trò quan trọng trong đời sống con người. Những hình ảnh bị chỉnh sửa được sử dụng cho mục đích xấu có thể dẫn đến những hậu quả không tốt. Trong khi đó, với sự sẵn có của các công cụ xử lý ảnh, ảnh số dễ dàng được thay đổi mà không để lại bằng chứng gì về thị giác. Để giải quyết vấn đề này và trả lời câu hỏi ảnh có độ tin cậy bao nhiêu, ảnh nào là thật, ảnh nào là giả, thì các kỹ thuật xác thực được phát triển. Chẳng hạn như kỹ thuật chủ động (active method) nhúng dấu thủy vân hay chữ ký số vào trong ảnh, ngược lại kỹ thuật thụ động (passive method) giúp phát hiện ảnh bị chỉnh sửa mà không cần dấu thủy vân hay chữ ký số được nhúng vào trước đó.

Có nhiều cách để tạo ra hình ảnh giả mạo, trong đó sao chép các vùng ảnh từ các ảnh khác nhau là một cách rất phổ biến. Trong khi làm như vậy, để tạo ra hình ảnh thuyết phục, người ta thường phải sửa kích thước, quay, hay co giãn các phần của ảnh, quá trình này đòi hỏi lấy mẫu lại (resampling). Mặc dù việc lấy mẫu lại thường không thể nhìn thấy bằng mắt thường nhưng nó vẫn để lại các dấu vết về mặt tương quan giữa các điểm ảnh. Vì vậy, dựa vào dấu vết của việc lấy mẫu lại để phát hiện ảnh giả mạo có các vùng được sao chép từ các nguồn khác nhau là một hướng nghiên cứu quan trọng, được nhiều người quan tâm.

Đầu tiên A.C. Popescu và H. Farid [7] trình bày phương pháp kiểm tra xem ảnh A có bị lấy mẫu lại hay không bằng cách sử dụng ma trận hệ số D kích thước $(2 \times M + 1) \times (2 \times M + 1)$ với M là hệ số, trong [4] gọi D là bộ dự báo (the prediction). Từ D xác định giá trị dự báo tại (i, j) theo công thức:

$$b_{ij} = \sum_{u=-M}^M \sum_{v=-M}^M d_{uv} \times a_{uv}$$

Hiệu giá trị dự báo và giá trị cho trước:

$$e_{ij} = b_{ij} - a_{ij}$$

gọi là sai số dự báo. Tiếp đó, tính $P_{ij} = P(a_{ij} = b_{ij})$ là xác suất để b_{ij} bằng a_{ij} . Các xác suất này tỷ lệ nghịch với sai số dự báo, nghĩa là e_{ij} càng nhỏ thì P_{ij} càng lớn và ngược lại. Ma trận P gồm các phần tử P_{ij} gọi là bản đồ xác suất (p-map). Các tác giả cũng chỉ ra rằng nếu A là ảnh bị lấy mẫu lại (resampled), thì tồn tại bộ dự báo D , sao cho các phần tử P_{ij} xấp xỉ bằng 1 xuất hiện một cách tuần hoàn. Để xác định D và P như vậy, Popescu

và Farid sử dụng phương pháp EM (Expectation Maximization). Tính tuần hoàn của P được nhận ra bằng cách sử dụng phổ của phép biến đổi Fourier rời rạc (DFT-Discrete Fourier Transform) đối với P . Trên phổ xuất hiện các điểm sáng nhọn (peaks) đối xứng xung quanh tâm là dấu hiệu chứng tỏ ảnh (hay vùng ảnh) đã bị lấy mẫu lại. Độ phức tạp của thuật toán xác định D và P trong [7] là lớn vì phải thực hiện các vòng lặp xác định hai ma trận này. Trong [4], Kirchner chỉ ra rằng D đóng vai trò không cao, nên để giảm thời gian tính toán, Kirchner đã chọn trước một ma trận hệ số D và tính ma trận bản đồ xác suất P theo D được chọn. Tuy nhiên, cả hai phương pháp [4] và [7] đều dựa trên sự quan sát các điểm sáng nhọn nên khó xác định được vùng giả mạo, vì vậy tính hiệu quả vẫn còn rất hạn chế.

Phát hiện lấy mẫu lại trên miền không gian được đề xuất trong [8] dựa trên tính sai phân bậc hai trên các hàng hoặc các cột của ma trận điểm ảnh. Phương pháp này có ưu điểm là tốc độ nhanh hơn phương pháp trong [4,7], tuy nhiên nó vẫn khó khoanh được vùng giả mạo. Trong [1] tác giả đã đưa ra một cải tiến nhỏ phương pháp trong [8] bằng cách sử dụng một giá trị ngưỡng với ma trận DFT của ma trận $p[k]$, nhưng cải tiến này cũng không nâng cao khả năng khoanh vùng phát hiện giả mạo.

R. Wang [11] đưa ra cách phát hiện dấu vết lấy mẫu lại trên ảnh bằng cách sử dụng phép biến đổi SVD (Singular Value Decomposition). Ảnh sau khi được lấy mẫu lại có đặc điểm là sự độc lập tuyến tính giữa các hàng và cột của ma trận điểm ảnh sẽ thay đổi, dùng phép biến đổi SVD để khảo sát sự thay đổi về sự độc lập tuyến tính, từ đó kết luận ảnh có giả mạo hay không. Phương pháp có ưu điểm là đơn giản nhưng chỉ đưa ra được kết luận ảnh có bị lấy mẫu lại hay không, chứ không phát hiện được các vùng giả mạo.

Trong [3] ba tác giả X. Feng, I. Cox, và G. Doerr tính mật độ năng lượng chuẩn hóa (normalized energy density) của các vùng ảnh để xác định giả mạo. Phương pháp dựa trên giả thiết là quá trình lấy mẫu lại sẽ ảnh hưởng đến sự phân bố năng lượng của ảnh trên

các miền tần số (frequency domain), trong đó năng lượng của ảnh được hiểu là tổng bình phương của các điểm ảnh ($E = \sum_{i,j} a_{ij}^2$). Cũng giống như [11] chỉ đưa ra được kết luận ảnh có lấy mẫu lại hay không.

Trong [8] ngoài trình bày phương pháp dựa trên sai phân bậc hai, S. Prasad và K. R. Ramakrishnan còn trình bày phương pháp sử dụng các phép biến đổi DCT và phép biến đổi DWT song trực giao 3.5 (biorthogonal 3.5) để xác định ảnh giả mạo có lấy mẫu tăng. Các phương pháp này có thể hiển thị được vùng giả mạo nhưng khối lượng tính toán bị dư thừa do phải tính toán cả những dữ liệu không sử dụng.

Hầu hết các phương pháp ở trên đều có nhược điểm như hiệu quả thấp, thời gian tính toán lớn, khó khoanh được vùng giả mạo. Phương pháp trong [8] sử dụng phép biến đổi DCT và DWT có ưu điểm hơn là khoanh được các vùng giả mạo. Trong bài báo này chúng tôi đề xuất hai phương pháp phát hiện ảnh giả mạo dựa trên phép biến đổi hiệu và lọc thông cao của phép biến đổi DWT. Các phương pháp này dựa trên tính phẳng của vùng ảnh được lấy mẫu tăng (mục III.3), có ưu điểm là đơn giản, định vị được các vùng giả mạo lấy mẫu tăng và bền vững trước một số phép biến đổi như quay, tịnh tiến, nén JPEG,... Các phương pháp đề xuất có khả năng phát hiện giả mạo tốt hơn phương pháp trong [4] của Kirchner và sai phân bậc hai trong [8], có khả năng phát hiện giả mạo tương đương với phương pháp sử dụng phép biến đổi DWT trong [8], nhưng có độ phức tạp tính toán thấp hơn.

Nội dung tiếp theo của bài báo được tổ chức như sau: Phần II trình bày một số phương pháp liên quan, Phần III trình bày tính chất của vùng ảnh sau khi lấy mẫu tăng và đưa ra một phép biến đổi mới trên ma trận, gọi là phép biến đổi hiệu, áp dụng phép biến đổi này để xây dựng phương pháp phát hiện ảnh giả mạo, Phần IV trình bày phương pháp dựa trên bộ lọc thông cao của phép biến đổi DWT, Phần V trình bày một số đánh giá và phân tích, Phần VI là kết quả thử nghiệm và Phần VII là kết luận.

II. MỘT SỐ PHƯƠNG PHÁP LIÊN QUAN

Mục này giới thiệu một số phương pháp phát hiện ảnh giả mạo, chúng được dùng để đánh giá, so sánh với các phương pháp đề xuất.

II.1 Phương pháp của Kirchner (ký hiệu là K4)

Trong [4], Kirchner sử dụng bộ dự báo cấp 3×3 như sau:

$$D = \begin{bmatrix} -0.25 & 0.5 & -0.25 \\ 0.5 & 0 & 0.5 \\ -0.25 & 0.5 & -0.25 \end{bmatrix}$$

Để phát hiện các vùng giả mạo của một ảnh, cần chia ảnh thành các khối cùng cấp $M \times N$ chồng lấn nhau (hai khối liên tiếp chỉ khác nhau một hàng hoặc một cột). Giả sử A là một khối cần xét, phương pháp kiểm tra tính giả mạo của A được thực hiện theo các bước:

Bước 1. Tính ma trận dự báo B của A bằng cách sử dụng bộ dự báo D theo công thức

$$B(u,v) = 0.5 \times [A(u,v-1) + A(u-1,v) + A(u,v+1) + A(u+1,v)] - 0.25 \times [A(u-1,v-1) + A(u-1,v+1) + A(u+1,v-1) + A(u+1,v+1)],$$

với $(u=2, \dots, M-1; v=2, \dots, N-1)$.

Bước 2. Tính ma trận sai số E :

$$E(u,v) = A(u,v) - B(u,v)$$

Bước 3. Tính ma trận P (p -map) theo công thức:

$$P(u,v) = \exp(-|E(u,v)|^2)$$

Bước 4. Thực hiện phép biến đổi DFT đối với ma trận P để được ma trận F .

Bước 5. Hiện thị F dưới dạng ảnh để quan sát. Nếu xuất hiện các điểm sáng nhọn (peaks) đối xứng xung quanh tâm thì kết luận khối A là giả mạo.

II.2 Phương pháp dựa trên sai phân bậc hai (ký hiệu là SPB2)

Trong [8], trình bày hai phương pháp dựa trên sai phân bậc hai. Cũng như phương pháp của Kirchner, ảnh được chia thành các khối cùng cấp chồng lấn nhau. Để kiểm tra tính giả mạo của khối A , cần thực hiện các bước:

Bước 1. Xây dựng ma trận nhị phân B ứng với A theo công thức:

$$B[u,v] = \begin{cases} 1 & \text{nếu } S[u,v] = 0 \\ 0 & \text{trái lại} \end{cases} \quad (1)$$

trong đó $S[u,v]$ là sai phân cấp hai tại $A[u,v]$ tính theo hàng. Nói cách khác:

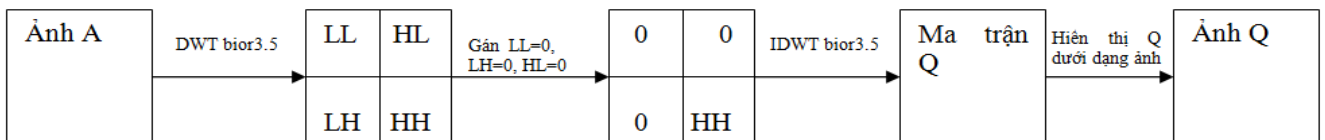
$$S[u,v] = A[u,v] + A[u,v+2] - 2A[u,v+1]$$

Bước 2. Thực hiện phép biến đổi DFT đối với ma trận B để được ma trận F .

Bước 3. Hiện thị F dưới dạng ảnh để quan sát. Nếu xuất hiện các điểm sáng nhọn đối xứng xung quanh tâm thì kết luận khối A là giả mạo.

Phương pháp thứ hai chỉ khác phương pháp thứ nhất cách xây dựng ma trận nhị phân B . Thay cho công thức (1) ở bước 1 bằng công thức:

$$B[u,v] = \begin{cases} 1 & \text{nếu } S[u,v] > 0 \text{ và } S[u,v+1] \leq 0 \\ 1 & \text{nếu } S[u,v] < 0 \text{ và } S[u,v+1] \geq 0 \\ 0 & \text{trái lại} \end{cases}$$



Hình 1. Sơ đồ các bước trong phương pháp dựa trên phép biến đổi DWT song trực giao 3.5 [8].

II.3 Phương pháp của Prasad và Ramakrishnan (ký hiệu là DWT3.5)

Trong [8], hai tác giả Prasad và Ramakrishnan còn đưa ra phương pháp phát hiện giả mạo dựa trên phép biến đổi DWT song trực giao 3.5, chi tiết các bước của phương pháp như sau: Đầu vào là một ảnh đa cấp xám I , có kích thước $2M \times 2N$.

Bước 1. Xây dựng ma trận điểm ảnh A từ I .

Bước 2. Biến đổi DWT với ma trận A được C gồm bốn vùng LL, LH, HL, HH như sau:

$$C = DWT(A) = \begin{bmatrix} LL & HL \\ LH & HH \end{bmatrix}_{34}$$

trong đó LL, LH, HL, HH là các ma trận con cấp $M \times N$. LL thường gọi là miền tần số thấp, LH, HL, HH là các miền tần số cao.

Bước 3. Trong C , thay LL, LH, HL bằng ma trận 0 cấp $M \times N$ được ma trận:

$$C' = \begin{bmatrix} 0 & 0 \\ 0 & HH \end{bmatrix}$$

Bước 4. Biến đổi IDWT được Q :

$$Q = IDWT(C')$$

Bước 5. Hiện thị ma trận Q dưới dạng ảnh, nhận thấy vùng ảnh không bị biến đổi sẽ sáng hơn và vùng ảnh giả mạo được lấy mẫu tăng sẽ tối hơn.

Các bước được mô tả theo sơ đồ trong Hình 1.

III. LẤY MẪU TĂNG VÀ PHÁT HIỆN ẢNH GIẢ MẠO BẰNG PHÉP BIẾN ĐỔI HIỆU

III.1 Lấy mẫu lại tín hiệu

Cho tín hiệu một chiều y gồm n mẫu: $y = (y_0, y_1, \dots, y_{n-1})$ và hệ số lấy mẫu lại α (với $\alpha > 1$: lấy mẫu tăng; $\alpha < 1$: lấy mẫu giảm). Khi đó có thể xem y như một hàm rời rạc xác định tại các tọa độ nguyên như Bảng 1.

Bảng 1. Tọa độ nguyên x và giá trị hàm y .

x	0	1	2	...	n-1
y	y_0	y_1	y_2	...	y_{n-1}

Quá trình lấy mẫu lại tín hiệu y gồm các bước như sau:

Bước 1. Biến đổi tọa độ từ nguyên sang thực.

Tọa độ nguyên $i=0, 1, \dots, n-1$ được biến đổi thành $\alpha \times i$, như Bảng 2 dưới đây:

Bảng 2. Tọa độ biến đổi từ x và giá trị hàm y .

X	0	α	$\alpha \times 2$	...	$\alpha \times (n-1)$
Y	y_0	y_1	y_2	...	y_{n-1}

Bước 2. Nội suy để xây dựng hàm liên tục $f(x)$ xác định trên đoạn $[0, \alpha \times (n-1)]$.

Bước 3. Xác định tín hiệu mới:

$$z_i = f(i)$$

với i nguyên, $i=0, \dots, (m-1)$ và $(m-1) = [\alpha \times (n-1)]$ (trong đó $[x]$ là phần nguyên dưới của x).

Ví dụ: Cho $\alpha=1.5$ và tín hiệu y như sau:

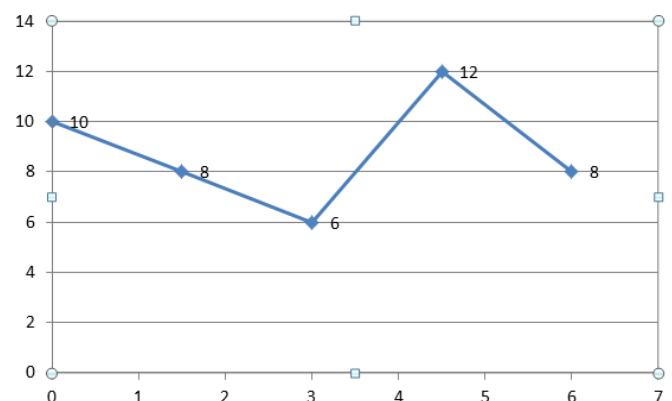
Bảng 3. Giá trị tọa độ nguyên x và giá trị hàm y .

x	0	1	2	3	4
y	10	8	6	12	8

Bước 1. Biến đổi tọa độ từ nguyên sang thực được Bảng 4.

Bảng 4. Giá trị tọa độ biến đổi từ x và giá trị hàm y .

x	0	1.5	3	4.5	6
y	10	8	6	12	8



Hình 2. Đồ thị của hàm $f(x)$.

Bước 3. Tạo tín hiệu mới $z_i = f(i)$ trong Bảng 5.

Bảng 5. Giá trị tín hiệu mới.

i	0	1	2	3	4	5	6
z _i	10	8.67	7.33	6	10	10.67	8

Các phần tử z_i chính là các giá trị mẫu của tín hiệu mới.

III.2 Lấy mẫu lại trên ảnh

Ảnh số là tín hiệu hai chiều (ma trận). Để lấy mẫu lại trên ảnh, đầu tiên tiến hành lấy mẫu lại từng hàng, sau đó lấy mẫu lại từng cột, kết quả được một ma trận ảnh mới. Khi hệ số lấy mẫu lại $\alpha > 1$ thì số mẫu (điểm ảnh) tăng lên, ảnh to hơn, trái lại nếu $\alpha < 1$ thì ảnh nhỏ đi. Kỹ thuật lấy mẫu lại thường được sử dụng để phóng to và thu nhỏ ảnh.

III.3 Tính chất của phép lấy mẫu tăng trên ảnh

Sau khi được lấy mẫu tăng (upsample) với tỉ lệ lấy mẫu $\alpha = p/q > 1$ thì ảnh rộng hơn (khoảng α^2 lần), số điểm ảnh (số mẫu) nhiều hơn, trong khi giá trị cực đại và cực tiểu của ảnh gần như không thay đổi, nên ảnh sẽ phẳng hơn (các điểm ảnh có giá trị đồng đều hơn).

Có thể đánh giá độ phẳng của ảnh bằng cách tính trung bình cộng (ký hiệu là T) giá trị tuyệt đối hiệu các cặp điểm ảnh kề nhau của ma trận điểm ảnh. Các giá trị điểm ảnh sau khi lấy mẫu tăng sẽ đồng đều hơn nên T này sẽ giảm đi. Để minh họa điều này chúng tôi thực hiện thử nghiệm trên 50 khối ảnh ngẫu nhiên có kích thước 8×8 , gọi là khối ảnh gốc. Các khối ảnh được lấy mẫu lại ở tỉ lệ $\alpha = p/q$ là 1.2; 1.5; 2 lần so với khối ảnh gốc, và sử dụng phương pháp nội suy: láng giềng gần nhất (Nearest Neighbor Interpolation), song tuyến tính (bilinear interpolation), song khối (Bicubic Interpolation). Biểu đồ mô tả kết quả thực hiện trên 50 khối như Bảng 6.

Qua các biểu đồ trong Bảng 6 nhận thấy đường màu tím chấm tròn thể hiện giá trị T của ma trận khối ảnh sau khi lấy mẫu tăng đều nằm bên dưới đường màu hồng chấm sao thể hiện giá trị T của ma trận khối ảnh ban đầu.

III.4 Phát hiện ảnh giả mạo bằng phép biến đổi hiệu

Trong phần này trình bày phép biến đổi hiệu trên ma trận điểm ảnh, và phương pháp phát hiện ảnh giả mạo dựa trên phép biến đổi hiệu.

III.4.1 Phép biến đổi hiệu trên ma trận điểm ảnh

Định nghĩa: Giả sử A là ma trận điểm ảnh cấp $2M \times 2N$, phép biến đổi hiệu trên A , ký hiệu $R = F_d(A)$, là ma trận cùng cấp với A được xác định như sau: Chia A thành các khối 2×2 theo thứ tự từ trái sang phải và từ trên xuống dưới. Sau đó biến đổi mỗi khối theo quy tắc:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \rightarrow \begin{bmatrix} \alpha & -\alpha \\ -\alpha & \alpha \end{bmatrix}, \alpha = \frac{1}{4}[(a+d) - (b+c)] \quad (2)$$

Nói cách khác, các phần tử của R được xác định theo công thức:

$$R_{2i-1,2j-1} = R_{2i,2j} = \frac{1}{4}((a_{2i-1,2j-1} + a_{2i,2j}) - (a_{2i-1,2j} + a_{2i,2j-1}))$$

$$R_{2i-1,2j} = R_{2i,2j-1} = -\frac{1}{4}((a_{2i-1,2j-1} + a_{2i,2j}) - (a_{2i-1,2j} + a_{2i,2j-1}))$$

$$\text{với: } i=1,2,\dots,M; j=1,2,\dots,N$$

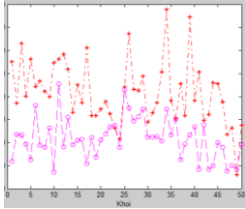
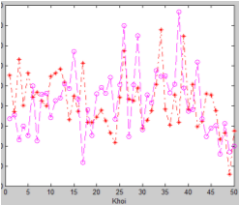
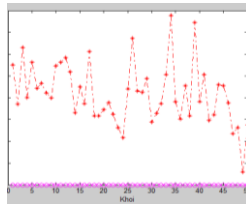
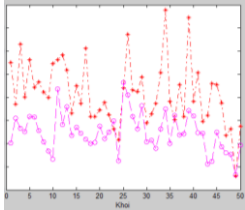
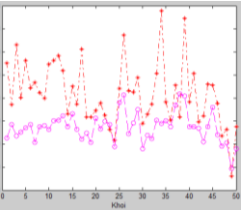
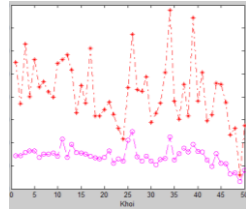
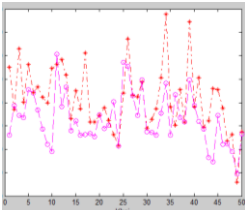
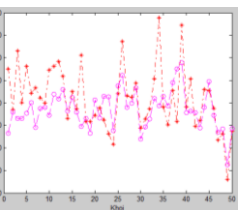
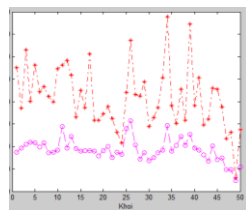
Từ định nghĩa có một số nhận xét sau đây.

Nhận xét 3.1: Nếu các phần tử trong khối con 2×2 của A có giá trị đồng đều (xấp xỉ bằng nhau) thì các phần tử trong khối con tương ứng $R = F_d(A)$ sẽ có giá trị tuyệt đối nhỏ gần bằng 0.

Ý tưởng của phương pháp phát hiện ảnh giả mạo: Giả sử I là ảnh cần kiểm tra. Nếu I có các vùng giả mạo, thì ma trận điểm ảnh A của nó có các khối con đồng đều về giá trị (tính chất mục III.3). Vì vậy, ma trận $R = F_d(A)$ sẽ có các khối có giá trị nhỏ gần bằng 0 (nhận xét 3.1). Khi hiển thị R thì các vùng giả mạo (ứng với các khối có giá trị nhỏ gần bằng 0) sẽ đen hơn các vùng khác. Dựa vào đặc điểm này dễ dàng định vị được các vùng giả mạo.

Chi tiết phương pháp được trình bày ở phần dưới đây.

Bảng 6. Kết quả mô tả độ đồng đều của các khối ảnh sau khi lấy mẫu tăng.

Tỷ lệ p/q	1.2	1.5	2
Láng giềng gần nhất			
Song tuyến tính			
Song khối			

III.4.2 Phương pháp phát hiện ảnh giả mạo dựa trên phép biến đổi hiệu (ký hiệu BDH)

Đầu vào là một ảnh đa cấp xám I .

Bước 1. Xây dựng ma trận điểm ảnh A từ I .

Bước 2. Tính:

$$R = F_d(A)$$

Bước 3: Hiển thị ảnh ứng với ma trận R . Vùng ảnh tối hơn chính là vùng giả mạo (vùng được tăng mẫu và dán vào ảnh gốc).

Nhận xét 3.2: Trong nhiều trường hợp ảnh có thể tồn tại các vùng tối nhưng không phải giả mạo, các vùng này xuất hiện một cách ngẫu nhiên, không có biên và không có ý nghĩa rõ ràng. Còn các vùng tối giả mạo sẽ có biên và có ý nghĩa. Tuy nhiên có một số trường hợp khác như chụp chỗ tối, chụp ban đêm, thì vẫn có thể xuất hiện các vùng tối có biên (khi hiển thị R), trường hợp này phương pháp đưa ra kết quả phát hiện nhầm (ảnh không giả mạo vẫn kết luận giả mạo). Đây là nhược điểm của các phương pháp đề xuất.

IV. ĐỀ XUẤT PHƯƠNG PHÁP DỰA TRÊN LỌC THÔNG CAO CỦA PHÉP BIẾN ĐỔI DWT

IV.1 Phép biến đổi DWT

Mỗi phép biến đổi Wavelet rời rạc sử dụng 2 bộ lọc (thường ký hiệu là L_0D và H_1D) để phân tích ảnh (Decomposition) gọi là quá trình thuận và 2 bộ lọc (thường ký hiệu là L_0R và H_1R) để dựng lại ảnh (Reconstruction) gọi là quá trình ngược, Ví dụ đối với phép biến đổi Wavelet rời rạc DB2, thì:

$$L_0D = [-0.1294, 0.2241, 0.8365, 0.4830],$$

$$H_1D = [-0.4830, 0.8365, -0.2241, -0.1294],$$

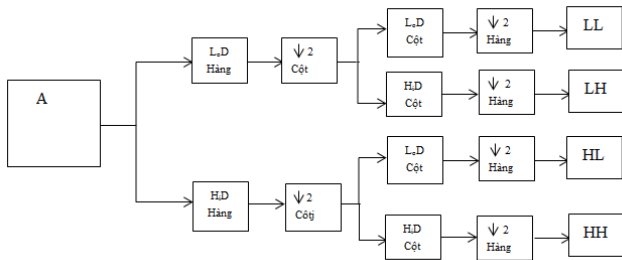
$$L_0R = [0.4830, 0.8365, 0.2241, -0.1294],$$

$$H_1R = [-0.1294, -0.2241, 0.8365, -0.4830].$$

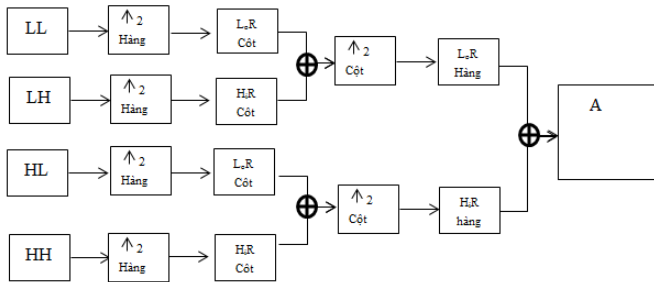
Để tiện theo dõi trong mục này chúng tôi trình bày lại phép biến đổi thuận DWT và ngược IDWT. Theo [6,9,10] phép biến đổi thuận và ngược DWT được thực hiện như sau:

Phép biến đổi thuận DWT 2 chiều: Phép biến đổi này sử dụng bộ lọc thông thấp L_oD để tính các giá trị vùng tần số thấp và lọc thông cao H_iD để tính các giá trị vùng tần số cao. Quá trình này được mô tả theo sơ đồ Hình 3.

Phép biến đổi ngược IDWT 2 chiều: Phép biến đổi này thực hiện theo trình tự ngược lại với phép biến đổi thuận, sử dụng bộ lọc thông thấp L_oR và lọc thông cao H_iR , cụ thể như sơ đồ Hình 4.



Hình 3. Sơ đồ thực hiện phép biến đổi DWT thuận.



Hình 4. Sơ đồ phép biến đổi DWT ngược.

Trong đó:

X Hàng	Cuộn theo hàng với bộ lọc X
X Cột	Cuộn theo cột với bộ lọc X
$\downarrow 2$ Hàng	Giảm mẫu 2 lần theo hàng: chỉ giữ lại các hàng có chỉ số lẻ (chỉ số tính từ 1).
$\downarrow 2$ Cột	Giảm mẫu 2 lần theo cột: chỉ giữ lại các cột có chỉ số lẻ.
$\uparrow 2$ Hàng	Tăng mẫu theo hàng: giữa 2 hàng thêm một hàng với các giá trị 0.
$\uparrow 2$ Cột	Tăng mẫu theo cột: giữa 2 cột thêm một cột với giá trị 0.
$\oplus$	Cộng hai ma trận cùng cấp.

IV.2 Đề xuất phương pháp giảm độ phức tạp tính toán (ký hiệu LTC)

Phương pháp DWT3.5 trong mục II.3 chỉ sử dụng ma trận con HH , trong khi đó vẫn phải tính toán các ma trận con LL , LH , HL . Như vậy độ phức tạp tính toán của phương pháp tăng mà không cần thiết. Trong phần dưới đây chúng tôi sẽ cải tiến phương pháp này để không phải tính toán dư thừa mà hiệu quả phát hiện vẫn tương đương.

Theo mục IV.1, để thực hiện phép biến đổi DWT cần sử dụng bộ lọc thông thấp và bộ lọc thông cao. Tương tự để thực hiện phép biến đổi IDWT cần sử dụng bộ lọc thông thấp và bộ lọc thông cao. Trong phương pháp đề xuất dưới đây trước tiên xây dựng ma trận con HH bằng cách chỉ sử dụng bộ lọc thông cao H_iD , sau đó phóng to HH để nhận được ma trận C (tương tự như ma trận Q) có cùng kích thước như ảnh ban đầu. Chi tiết các bước của phương pháp như sau:

Đầu vào là một ảnh đa cấp xám I , có kích thước $2M \times 2N$.

Bước 1. Xây dựng ma trận điểm ảnh A từ I .

Bước 2. Sử dụng bộ lọc thông cao H_iD cuộn theo hàng cho ma trận A để nhận được ma trận L có kích thước $2M \times N$.

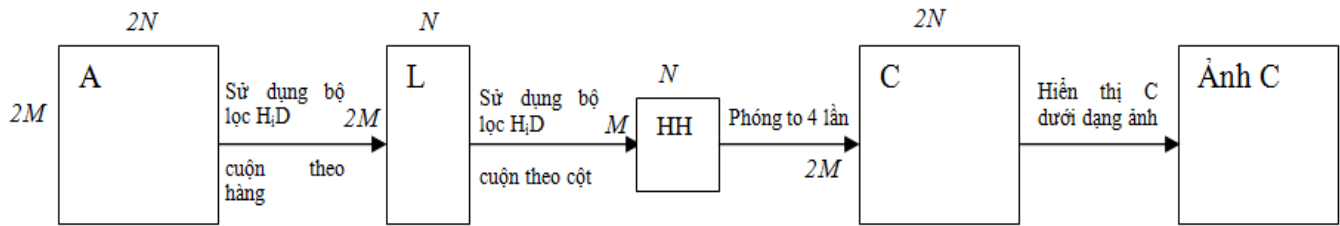
Bước 3. Sử dụng bộ lọc thông cao H_iD cuộn theo cột cho ma trận L được HH có kích thước $M \times N$.

Bước 4. Phóng to HH lên 4 lần để nhận được C có kích thước $2M \times 2N$. Trong phép phóng to này, mỗi phần tử HH_{ij} tạo ra một ma trận con cấp 2×2 , như sau:

$$HH_{ij} \rightarrow \begin{bmatrix} \alpha & -\alpha \\ -\alpha & \alpha \end{bmatrix} \text{ với: } \alpha = HH_{ij}$$

Bước 5. Hiện thị ma trận C dưới dạng ảnh, nhận thấy vùng ảnh không bị biến đổi sẽ sáng hơn và vùng ảnh giả mạo được lấy mẫu tăng sẽ tối hơn.

Các bước được mô tả theo sơ đồ trong Hình 5 bên dưới.



Hình 5. Sơ đồ các bước trong phương pháp LTC.

Nhận xét:

- Thay vì tính đầy đủ quá trình DWT và IDWT thì phương pháp đề xuất sử dụng bộ lọc thông cao H_iD chỉ tính các dữ liệu cần thiết để có vùng HH , sau đó phóng to 4 lần thay vì sử dụng phép IDWT, nên phương pháp có độ phức tạp thấp hơn đáng kể so với phương pháp DWT3.5.

- Theo [trang 66-67,6], khi áp dụng lọc thông cao với các vùng ảnh càng phẳng (smooth) thì sẽ nhận được các giá trị càng gần 0 hơn. Nên các khối con của HH ứng với các miền giả mạo sẽ có các giá trị gần 0 hơn so với các miền khác. Vì vậy, hiển thị HH cũng phát hiện được các vùng giả mạo. Như vậy, bước 4 áp dụng IDWT trong DWT3.5 chỉ có vai trò phóng to vùng HH để định vị vùng giả mạo ứng với ảnh gốc. Tương tự, trong phương pháp LTC chúng tôi sử dụng phép phóng to 4 lần cũng có thể định vị được các vùng giả mạo. Ngoài ra, phép phóng to này độ phức tạp tính toán thấp hơn so với phép IDWT và trong nhiều trường hợp nhận được các vùng giả mạo rõ nét hơn.

V. ĐÁNH GIÁ ĐỘ PHỨC TẠP TÍNH TOÁN VÀ TÍNH BỀN VỮNG CỦA CÁC PHƯƠNG PHÁP

V.1 Đánh giá độ phức tạp tính toán của phương pháp BDH

Trong phương pháp biến đổi hiệu BDH có bước 2 quá trình áp dụng phép biến đổi hiệu cho ma trận ảnh A là chính nên để đánh giá độ phức tạp ta chỉ cần đánh giá các bước này.

Theo công thức (2) để biến đổi 1 khối 2×2 cần: 2 phép cộng, 1 phép trừ và 1 phép chia cho 4 (có thể

thay bằng phép dịch chuyển 2 bit), như vậy cần 4 phép tính.

Đối với ảnh có kích thước $2M \times 2N$ thì số khối cần biến đổi $M \times N$, nên độ phức tạp tính toán của phương pháp BDH sẽ là:

$$T(BDH) = 4 \times M \times N$$

V.2 Đánh giá độ phức tạp tính toán của phương pháp DWT3.5

Để áp dụng phép cuộn với bộ lọc có kích thước S cho mỗi phần tử trong hàng/cột thì cần: S phép nhân và $S-1$ phép cộng. Nên với một hàng gồm $2N$ phần tử sẽ cần: $2N \times (S+S-1)$ phép toán hoặc với một cột $2M$ phần tử sẽ cần $2M \times (S+S-1)$ phép toán.

Trong phương pháp DWT3.5 thì bước 2 áp dụng phép biến đổi DWT và bước 4 áp dụng phép biến đổi IDWT là chính nên để đánh giá độ phức tạp ta chỉ cần đánh giá các bước này.

Theo bước 2 với phép biến đổi DWT cần áp dụng bộ lọc L_oD , H_iD để cuộn ma trận A và sau đó tiếp tục dùng 2 bộ lọc này cuộn 2 ma trận có số chiều $2M \times N$ cho ra các vùng LL , LH , HL , HH , nên sẽ cần số phép tính:

$$2 \times (2M \times 2N \times (S+S-1)) + 4 \times (2M \times N \times (S+S-1))$$

Tương tự như vậy bước 4 với phép biến đổi IDWT có độ phức tạp như quá trình DWT và thêm $8 \times M \times N$ phép toán cho 3 phép cộng ma trận cùng cấp.

Vậy độ phức tạp tính toán của DWT3.5 là:

$$\begin{aligned} T(DWT3.5) &= 2 \times (2 \times (2M \times 2N \times (S+S-1)) + \\ &\quad 4 \times (2M \times N \times (S+S-1))) + 8 \times M \times N \\ &= 32 \times (M \times N \times (S+S-1)) + 8 \times M \times N \end{aligned}$$

V.3 Đánh giá độ phức tạp tính toán của phương pháp LTC

Với phương pháp LTC thì bước 2 và bước 3 chỉ áp dụng bộ lọc thông cao H_D để tính HH là chính và đáng kể.

Bước 2 sẽ cần số phép toán là:

$$2M \times 2N \times (S+S-1)$$

Bước 3 sẽ cần số phép toán là:

$$2M \times N \times (S+S-1).$$

Vì không phải thực hiện quá trình IDWT nên độ phức tạp tính toán của LTC sẽ là:

$$\begin{aligned} T(LTC) &= 2M \times 2N \times (S+S-1) + 2M \times N \times (S+S-1) \\ &= 6 \times (M \times N \times (S+S-1)) \end{aligned}$$

Để tiện so sánh độ phức tạp tính toán của các phương pháp chúng tôi lập Bảng 7 tổng hợp dưới đây:

Bảng 7. Độ phức tạp tính toán của các phương pháp.

Phương pháp	Độ phức tạp
BĐH	$4 \times M \times N$
DWT3.5	$32 \times (M \times N \times (S+S-1)) + 8 \times M \times N$
LTC	$6 \times (M \times N \times (S+S-1))$

Nhận xét:

- Qua Bảng 7 tổng hợp trên có thể nhận thấy:
- + Phương pháp BĐH có độ phức tạp thấp nhất.
- + Phương pháp DWT3.5 có độ phức tạp cao nhất.
- + Phương pháp LTC có độ phức tạp bằng khoảng 1/6 phương pháp DWT3.5.
- Do độ phức tạp của các phương pháp DWT3.5, LTC đều có thành phần S là số phần tử của các bộ lọc, nếu bộ lọc có kích thước lớn thì độ phức tạp tính toán của các phương pháp sẽ tăng và ngược lại. Trường hợp phương pháp DWT3.5 và LTC sử dụng phép biến đổi DWT song trực giao 3.5 thì bộ lọc có kích thước $S=12$, khi đó độ phức tạp của $T(DWT3.5) = 744 \times M \times N$, $T(LTC) = 138 \times (M \times N)$, như vậy $T(LTC) \approx 1/6 T(DWT3.5)$. Trong thực nghiệm, thời gian

thực hiện DWT3.5 thường lớn hơn thời gian thực hiện LTC từ 6 đến 7 lần.

V.4 Phân tích tính bền vững của các phương pháp

Đối với phép quay, tịnh tiến: Các phép biến đổi này có đặc điểm không làm thay đổi giá trị mà chỉ thay đổi vị trí điểm ảnh nên không ảnh hưởng đến tính phẳng ban đầu của ảnh.

Đối với phép nhiễu, làm mờ,...: Bản chất của các phép biến đổi này là thêm một giá trị nhiễu vào các điểm ảnh. Nếu các giá trị nhiễu nhỏ (hệ số thấp) thì không làm thay đổi giá trị điểm ảnh nhiều nên vẫn giữ được tính phẳng ban đầu của ảnh.

Đối với phép nén JPEG: Nén JPEG là nén mất mát thông tin, có thể làm thay đổi giá trị điểm ảnh. Tuy nhiên, nếu nén với tỷ lệ không quá lớn thì các giá trị thay đổi ít, nên vẫn giữ được tính phẳng ban đầu của ảnh.

Như vậy, các phép biến đổi trên đều không làm ảnh hưởng nhiều đến tính phẳng ban đầu của ảnh. Trong khi đó, các phương pháp DWT3.5 và các phương pháp đề xuất BĐH, LTC đều dựa trên tính chất phẳng của ảnh sau khi được lấy mẫu tăng, nên có khả năng bền vững trước các phép biến đổi này.

VI. KẾT QUẢ THỬ NGHIỆM

Mục này sẽ minh họa khả năng phát hiện giả mạo, tính bền vững, thời gian thực hiện và đánh giá các khả năng này bằng thực nghiệm trên tập 100 ảnh lấy ngẫu nhiên từ thư viện chuẩn UCID (*Uncompressed Colour Image Database*, <http://homepages.lboro.ac.uk/~cogs/datasets/ucid/ucid.html>). Chương trình thử nghiệm được viết trên môi trường Matlab 2011, và máy tính có cấu hình chip Intel 2×2.2 GHz, RAM 3 GB.

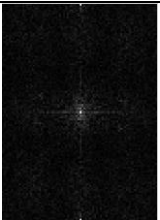
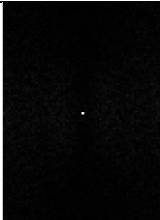
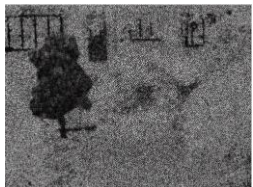
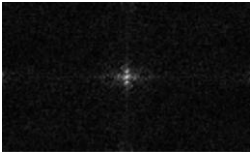
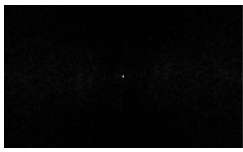
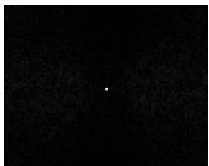
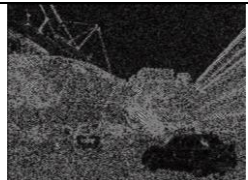
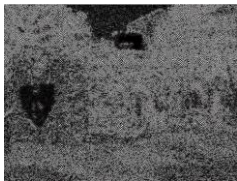
VI.1 Một số hình ảnh minh họa khả năng các phương pháp

Để minh họa khả năng của các phương pháp chúng tôi chọn một số hình ảnh đã được làm giả (vùng khoanh tròn) trong Bảng 8.

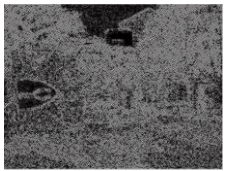
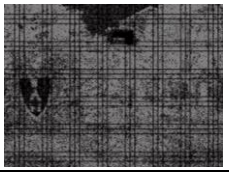
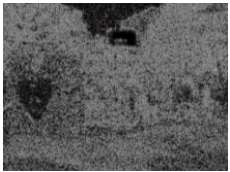
Bảng 8. Một số hình ảnh giả mạo được dùng để thực nghiệm.

			
Ảnh giả mạo 1	Ảnh giả mạo 2	Ảnh giả mạo 3	Ảnh giả mạo 4

Bảng 9. Một số hình ảnh giả mạo và kết quả phát hiện.

K4	SPB2	DWT3.5	LTC	BĐH
				
				
				
				

Bảng 10. Minh họa tính bền vững của các phương pháp

Ảnh giả mạo 4	DWT3.5	LTC	BDH
Quay 45 ⁰			
Quay 90 ⁰			
Co giãn ảnh 10%			
Nén JPEG Q=60			

Bảng 11. Thời gian thực hiện của 3 phương pháp (đơn vị là giây).

Tên ảnh	DWT3.5	LTC	BDH
Ảnh giả mạo 1	0.06873153	0.01234781	0.01023203
Ảnh giả mạo 2	0.07134330	0.01149425	0.01021168
Ảnh giả mạo 3	0.06715074	0.01137544	0.01012858
Ảnh giả mạo 4	0.06705382	0.01158946	0.01020247

Bảng 12. Đánh giá khả năng phát hiện và tính bền vững của các phương pháp.

Tên phương pháp	Chưa tấn công	Co giãn ảnh		Quay vùng giả mạo			Nén JPEG		
		5%	10%	45 ⁰	90 ⁰	180 ⁰	Q = 60	Q = 75	Q = 90
DWT3.5 và LTC	89	85	82	70	82	82	75	84	89
BDH	86	80	76	68	79	80	77	81	86

Bảng 9 là một số minh họa kết quả phát hiện của các phương pháp. Qua bảng này nhận thấy các hình ảnh của DWT3.5, BDH, LTC được khoanh vùng giả mạo một cách rõ nét và phân biệt với các vùng còn lại.

Trong khi đó các phương pháp K4 và SPB2 mặc dù xét trường hợp thuận lợi nhất: chọn khối nằm trong vùng giả mạo, nhưng dấu hiệu giả mạo (các điểm sáng nhon đối xứng xung quanh tâm) vẫn không hiển thị

một cách rõ ràng. Điều đó cho thấy khả năng phát hiện giả mạo của hai phương pháp này rất thấp, vì vậy trong phần thử nghiệm tiếp theo chỉ xét 3 phương pháp còn lại.

Bảng 10 là một số minh họa kết quả phát hiện của các phương pháp với Ảnh giả mạo 4 sau khi thực hiện một số phép tấn công như quay ảnh, co giãn, nén JPEG.

Trong Bảng 11 là kết quả so sánh thời gian thực hiện của ba phương pháp DWT3.5, LTC, BDH với 4 ảnh minh họa trong Bảng 3, các ảnh đều có kích thước 512×384 .

Nhận xét:

- Phương pháp BDH có thời gian thực hiện ít nhất, DWT3.5 có thời gian thực hiện lớn nhất, và thời gian thực hiện của DWT3.5 gấp khoảng 6 lần thời gian thực hiện của LTC. Điều này hoàn toàn phù hợp với đánh giá và phân tích lý thuyết ở mục V.

- Trong thực tế khi kiểm tra ảnh giả mạo sẽ phải thực hiện chia ảnh thành các khối chồng lấn nhau và kiểm tra trên từng khối. Số khối này rất lớn nên cải tiến giảm độ phức tạp tính toán sẽ giúp việc thực hiện chạy chương trình nhanh hơn.

VI.2 Đánh giá và so sánh hiệu quả các phương pháp

Để đánh giá hiệu quả và so sánh các phương pháp chúng tôi thử nghiệm trên 100 ảnh được chọn lựa ngẫu nhiên từ thư viện chuẩn UCID, sau đó các ảnh này được chuyển sang đa cấp xám. Để tạo ra ảnh giả mạo chúng tôi sử dụng phần mềm Photoshop chỉnh sửa.

Trong Bảng 11 là kết quả phát hiện trên tập ảnh thử nghiệm được chỉnh sửa với vùng giả mạo chèn vào có tỉ lệ lấy mẫu $p/q=2$, gồm hai trường hợp là không tấn công và có tấn công ảnh với các phép như: co giãn ảnh, quay, nén JPEG.

Bảng 11 cho thấy tỉ lệ bỏ sót tương đối thấp, và có tỉ lệ phát hiện cao với ảnh giả mạo bị tấn công. Các phương pháp DWT3.5, BDH, LTC đều dựa trên tính

chất phẳng của ảnh sau khi được lấy mẫu tăng, trong khi hầu hết các phép biến đổi như quay, co giãn, nén JPEG,... gần như không làm ảnh hưởng đến tính phẳng này, nên các phương pháp bền vững trước các phép biến đổi. Kết quả thực nghiệm cũng cho thấy phương pháp DWT3.5 và LTC có tỉ lệ phát hiện tương đương.

VII. KẾT LUẬN

Trong bài báo này, chúng tôi đề xuất hai phương pháp phát hiện ảnh giả mạo dựa trên phép biến đổi hiệu và lọc thông cao của phép biến đổi DWT. Qua phân tích, đánh giá và thực nghiệm cho thấy, so với các phương pháp K4 trong [4] và phương pháp SPB2 trong [1,8] thì các phương pháp mới có khả năng phát hiện tốt hơn hẳn, thực tế thì các phương pháp K4, SPB2 có khả năng phát hiện rất thấp. So với phương pháp DWT 3.5 trong [8], các phương pháp mới có độ phức tạp tính toán thấp hơn, và trong một số trường hợp có khả năng khoanh vùng và thể hiện vùng giả mạo rõ ràng, sắc nét hơn. Các phương pháp mới cũng bền vững hơn trước một số phép biến đổi ảnh, điều này được chúng tôi chứng minh và phân tích dựa trên tính phẳng của ảnh sau khi được lấy mẫu tăng mà [8] vẫn chưa chỉ ra được.

TÀI LIỆU THAM KHẢO

- [1] G. K. BIRAJDAR, V. H. MANKAR, "Blind Authentication of Resampled Images and Rescaling Factor Estimation", Proceedings of the IEEE International Conference on Cloud & Ubiquitous Computing & Emerging Technologies, 2013.
- [2] I. DAUBECHIES, *Ten lectures on wavelets*, Society for Industrial and Applied Mathematics Philadelphia, PA, USA, 1992.
- [3] X. FENG, I. COX, and G. DOERR, "Normalized energy density based forensic detection of resampled images", IEEE Trans. Inf. Forensics Security, vol. 14, no. 3, pp. 536–545, June 2012.

- [4] M. KIRCHNER, "Fast and reliable resampling detection by spectral analysis of fixed linear predictor residue", Proceedings of the 10th ACM Workshop on Multimedia and Security - MM&Sec 2008, 2008.
- [5] S. MALLAT, *A Wavelet Tour of Signal Processing*, 2nd ed. San Diego, CA: Academic, 1999.
- [6] ALASDAIR MCANDREW, *Introduction to Digital Image Processing with MATLAB*, Course Technology/Thompson Learning, 2004.
- [7] A. C. POPESCU and H. FARID, "Exposing digital forgeries by detecting traces of re-sampling", IEEE Transactions on Signal Process. , vol. 53, no. 2, pp. 758-767, Feb. 2005.
- [8] S. PRASAD, K. R. RAMAKRISHNAN, "On resampling detection and its application to image tampering", Proc. IEEE Int. Conf. Multimedia Expo., Toronto, Canada, pp. 1325-1328, 2006.
- [9] D. SALOMON, *Data Compression: The Complete Reference*, 3rd ed., Springer, 2004.
- [10] G. STRANG, T. NGUYEN, *Wavelets and filter banks*, Wellesley-Cambridge Press, 1996.
- [11] R. WANG, P. XIJIAN, "Detection of Resampling Based on Singular Value Decomposition", in Proceedings 5th International Conference on Image and Graphics, Xi'an, China, pp. 879-884, Sep 21 2009.

Ngày nhận bài: 18/9/2015

SƠ LƯỢC VỀ TÁC GIẢ

TRẦN ĐĂNG HIỀN



Sinh ngày 06/08/1983 tại Hà Nội.

Tốt nghiệp ĐH năm 2005, Thạc sĩ năm 2010 tại Trường ĐH Công nghệ – ĐH Quốc gia Hà Nội. Giảng dạy tại Trường ĐH Công nghệ - ĐH Quốc gia Hà Nội.

Lĩnh vực nghiên cứu: Giảu tin, thủy văn số, phát hiện ảnh giả mạo.

Email: hientd_68@yahoo.com

PHẠM VĂN ÁT



Sinh ngày 12/6/1945 tại Hà Nội.

Tốt nghiệp ĐH năm 1967 và tiến sĩ năm 1980 tại Trường ĐH Tổng hợp Hà Nội. Năm 1984 nhận học hàm Phó Giáo sư.

Hiện giảng dạy tại Khoa CNTT – Trường ĐH Giao thông Vận tải Hà Nội.

Lĩnh vực nghiên cứu: Lý thuyết ma trận, xử lý ảnh, an toàn thông tin, phân tích dữ liệu.

Email: phamvanat83@vnn.vn

NGUYỄN NGỌC HƯNG



Ngày sinh 9/12/1987 tại Hưng Yên

Tốt nghiệp ĐH năm 2009, Thạc sĩ năm 2014.

Hiện là nghiên cứu viên tại Phòng Tin học Viễn thông, Viện CNTT, viện Hàn lâm Khoa học Công nghệ

Việt Nam.

Lĩnh vực nghiên cứu: Giảu tin, thủy văn số, xử lý ảnh, mạng máy tính

Email: nnhung@ioit.ac.vn