

Giấu tin thuận nghịch sử dụng các thuộc tính của ngữ cảnh dự báo để loại bỏ bản đồ định vị

Nguyễn Kim Sao¹, Đỗ Văn Tuấn², Phạm Văn Ất¹

¹Khoa Công nghệ Thông tin, Trường Đại học Giao thông Vận tải

²Khoa Công nghệ Thông tin, Trường Đại học Công nghiệp Hà Nội

Tác giả liên hệ: Nguyễn Kim Sao, saonkoliver@utc.edu.vn

Ngày nhận bài: 03/10/2017, ngày sửa chữa: 04/07/2018, ngày duyệt đăng: 12/10/2018

Xem sớm trực tuyến: 28/12/2018, định danh DOI: 10.32913/rd-ict.vol3.no40.598

Biên tập lĩnh vực điều phối phản biện và quyết định nhận đăng: TS. Nguyễn Thái Sơn

Tóm tắt: Bài báo trình bày một lược đồ giấu tin thuận nghịch mới sử dụng phương pháp dự báo hình thoi. Các điểm ảnh được chia thành hai tập hợp: tập chấm và tập chéo. Tập chéo được sử dụng làm ngữ cảnh dự báo cho mỗi điểm của tập chấm. Tập chấm được dùng để nhúng tin theo phương pháp mở rộng sai số dự báo. Hai đại lượng có tính chất bất biến đối với quá trình nhúng là phương sai địa phương và độ sâu của ngữ cảnh dự báo trong miền giá trị dữ liệu ảnh ($[0, 255]$ đối với ảnh đa mức xám) được sử dụng để sắp xếp các điểm ảnh của tập chấm. Kết quả nhận được là các đoạn khả mở (chứa toàn các điểm có thể mở rộng như ở trên). Mỗi đoạn khả mở được định vị bởi hai số nguyên có độ dài 16 bit. Dùng tối đa 10 đoạn có thể đủ để bao gồm hầu hết các điểm khả mở, tương đương 320 bit bổ trợ. Nhờ vậy, phương pháp đề xuất có thể cải thiện khả năng nhúng cũng như chất lượng ảnh do không cần dùng bản đồ định vị như các phương pháp trước đó.

Từ khóa: *Giấu tin thuận nghịch, sắp xếp điểm ảnh, mở rộng hiệu, dự báo điểm ảnh.*

Title: **Reversible Data Embedding without Location Map using Prediction Context Properties**

Abstract: This paper presents a new reversible data hiding scheme based on rhombus prediction. Pixels are divided into two sets: dots and crosses. The set of crosses is used as the prediction context for each pixel of the dots. The set of dots is used to embed the message using prediction error expansion. Local variance and depth of the prediction context in the image-value domain ($[0, 255]$ for grayscale images), which are two unchanged attributes in the embedding process, are used to sort the pixels of the set of dots. From this sorted set, we obtain the expandable segments (containing only the expandable pixels). Each expandable segment is marked by two 16-bit integers. Using at most 10 segments, equivalent to 320 extra bits, may be sufficient to cover all expandable bits for hiding data. As a result, the proposed method can improve the embedding capacity as well as the image quality without using the location map as in previous methods.

Keywords: *Reversible data hiding, pixel sorting, difference expansion, pixel prediction.*

I. GIỚI THIỆU

Sự phát triển không ngừng của Internet mang lại những lợi ích vô cùng to lớn cho sự trao đổi thông tin của con người. Tri thức và các ứng dụng cũng vì thế mà ngày càng dễ dàng được tiếp cận hơn. Nhiều sản phẩm, đặc biệt là các sản phẩm đa phương tiện được công khai hoặc truyền thông trên Internet. Việc đó dẫn đến sự lợi dụng của những kẻ vi phạm bản quyền, thực hiện các hành vi như ăn cắp hay xuyên tạc thông tin. Để góp phần ngăn chặn vấn nạn đó, các phương pháp giấu tin và thủy vân số đã ra đời. Tuy nhiên, các phương pháp giấu tin và thủy vân truyền thống không cho phép khôi phục được ảnh gốc, nên không đáp ứng được nhiều ứng dụng nhất là trong các lĩnh vực quốc phòng, an ninh, y tế và giáo dục. Do đó, một hướng

nghiên cứu mới, giàu tiềm năng đã xuất hiện, đó là giấu tin và thủy vân thuận nghịch (reversible) [1, 2] hay bảo toàn (lossless) [3, 4]. Các phương pháp này, ngoài việc trích tin nhúng còn cho phép khôi phục lại ảnh gốc ban đầu. Thủy vân thuận nghịch thường được dùng để xác thực tính toàn vẹn của ảnh.

Trong [3], Macq đề xuất phương pháp thủy vân thuận nghịch dựa trên phép cộng modulo 256, tuy nhiên phương pháp này cho chất lượng ảnh không cao. Không lâu sau, Fridrich và các cộng sự trong [5] đề xuất một phương pháp thủy vân thuận nghịch sử dụng kỹ thuật nén bảo toàn dữ liệu. Ở phương pháp này, các bit thấp của mỗi điểm ảnh được nén lại để tạo ra không gian trống dùng để nhúng thủy vân. Đến nay đã có thêm nhiều phương pháp giấu tin

và thủy văn thuận nghịch, như dịch chuyển histogram [6], lượng tử hóa [7], mở rộng hiệu (DE: Difference Expansion) [8], kết hợp các phương pháp [9], hay gần đây là giấu tin và thủy văn thuận nghịch dựa vào dự báo kết hợp với các phương pháp trên [2, 9, 10]. Các nghiên cứu phát triển kỹ thuật giấu tin thuận nghịch thường hướng tới hai mục tiêu là khả năng nhúng và chất lượng ảnh chứa tin.

Với các phương pháp mở rộng hiệu, chất lượng ảnh sau khi nhúng phụ thuộc độ lệch của hai điểm ảnh (hiệu) được xét, bởi vậy hiệu càng nhỏ thì chất lượng ảnh càng tốt. Ở đề xuất đầu tiên bởi Tian [8], hiệu được xét là hiệu của cặp hai điểm ảnh kề nhau, các cặp điểm này sẽ được phân thành hai loại: khả mở và không khả mở (được nêu chi tiết tại mục II-1). Mỗi cặp khả mở được dùng để nhúng một bit, trong khi đó các cặp không khả mở bị bỏ qua. Để lưu trữ thông tin về tính chất khả mở hay không khả mở của mỗi cặp, Tian sử dụng một dãy nhị phân có độ dài bằng số cặp điểm ảnh: cặp khả mở ứng với bit 1, không khả mở ứng với bit 0. Dãy bit nhị phân này gọi là bản đồ định vị, được sử dụng ở giai đoạn trích bit thủy văn và khôi phục ảnh gốc, vì vậy nó cần được nhúng cùng dãy bit dữ liệu vào các cặp khả mở của ảnh gốc. Do độ dài của bản đồ định vị khá lớn, nên cần sử dụng một kỹ thuật nén bảo toàn như mã loạt (run-length coding) hoặc mã số học (arithmetic coding). Như vậy, khả năng nhúng cực đại của lược đồ này bằng số cặp điểm khả mở trừ đi độ dài của dữ liệu nén của bản đồ định vị. Giả sử (x, y) là một cặp điểm ảnh $(x, y \in [0, 255])$ đối với ảnh đa mức xám), $h = x - y$ là hiệu của chúng và (x', y') là cặp điểm nhận được sau khi nhúng 1 bit bằng phương pháp DE thì các sai khác giữa x' và x và giữa y' và y đều xấp xỉ bằng h (xem mục II-1). Rõ ràng là, nếu hiệu h càng nhỏ thì mức độ khả mở của (x, y) càng lớn và chất lượng ảnh đã giấu tin càng cao.

Để có được các hiệu nhỏ, các công trình gần đây [1, 2, 11] đã thay việc xét hiệu giữa hai cặp điểm bằng hiệu giữa một điểm và giá trị dự báo của nó. Hiệu này thường nhỏ vì giá trị dự báo thường gần bằng giá trị của điểm gốc. Các phương pháp này gọi là mở rộng sai số dự báo (PEE: Prediction-Error Expansion). Việc xét các sai số dự báo không những cho các hiệu nhỏ mà số hiệu nhận được còn tăng gấp đôi so với phương pháp của Tian vì mỗi điểm ảnh đều có thể được dự báo. Khả năng nhúng tin vẫn bằng số điểm khả mở trừ đi độ dài mã nén của bản đồ định vị, nhưng sẽ được cải thiện đáng kể vì số điểm khả mở so với trước tăng lên.

Để nâng cao khả năng nhúng tin, Sachnev và các cộng sự trong [10] đề xuất một phương pháp nhằm loại bỏ bản đồ định vị. Phương pháp này dựa trên nhận xét: Ngưỡng cảnh dự báo của một điểm ảnh càng phẳng (smooth hoặc flat), thì sai số dự báo càng nhỏ và điểm ảnh càng có xu hướng khả mở. Tính phẳng của ngưỡng cảnh dự báo được các tác giả

đánh giá thông qua phương sai địa phương của nó (xem mục II-3): Phương sai này càng nhỏ thì độ phẳng càng tăng và xác suất khả mở càng lớn. Trên cơ sở đó, Sachnev và cộng sự tiến hành sắp xếp các điểm ảnh theo thứ tự tăng của phương sai địa phương để dồn hầu hết các điểm khả mở lên đầu.

Tuy nhiên, tính khả mở của một điểm còn phụ thuộc vào một yếu tố quan trọng khác, đó là vị trí của ngưỡng cảnh dự báo so với miền giá trị điểm ảnh $[0, 255]$. Có thể dễ dàng nhận thấy, nếu ngưỡng cảnh dự báo càng nằm sâu trong miền giá trị điểm ảnh thì khả năng khả mở của điểm ảnh càng cao (xem mục II-1). Một cách ngắn gọn, đặc trưng này được gọi là độ sâu của ngưỡng cảnh và được đo bằng hiệu số giữa tâm của ngưỡng cảnh và tâm của miền điểm ảnh (là 128). Tại mục III-1 chúng tôi đưa ra ví dụ cụ thể để minh họa vai trò của vị trí ngưỡng cảnh dự báo đối với tính khả mở. Trong bài báo này chúng tôi đề xuất việc khai thác đặc tính độ sâu cùng với phương sai địa phương để tăng tính hiệu quả của phương pháp sắp xếp. Bằng cách đó chúng ta có thể thu được dãy điểm khả mở dài hơn so với phương pháp của Sachnev và cộng sự (xem mục IV-1). Ngoài ra, chúng tôi cũng đề xuất việc sử dụng các đoạn khả mở để nhúng tin mà không cần dùng bản đồ định vị (xem mục III-2).

Kết quả thực nghiệm đã cho thấy phương pháp đề xuất có khả năng nhúng tin cao hơn so với các phương pháp của Sachnev và cộng sự (gọi tắt là Sachnev) [10] và các phương pháp gần đây như: phương pháp của Qu và Kim (gọi tắt là Qu) [11], phương pháp của Kumar và Agrawal (gọi tắt là Kumar) [2].

Nội dung các phần tiếp theo của bài báo được tổ chức như sau: Mục II giới thiệu các công trình liên quan, mục III trình bày phương pháp đề xuất, mục IV so sánh phương pháp đề xuất với các phương pháp liên quan, và cuối cùng là kết luận ở mục V.

II. NHỮNG CÔNG TRÌNH LIÊN QUAN

1. Phương pháp mở rộng hiệu

Phương pháp mở rộng hiệu (DE: Difference Expansion) được đề xuất bởi Tian [8] vào năm 2003. Từ đó đến nay, phương pháp này liên tục được quan tâm và cải tiến do tiềm năng phát triển của nó.

1) Giấu tin theo phương pháp mở rộng hiệu:

Để nhúng một bit $b \in \{0, 1\}$ vào cặp điểm ảnh (x, y) , phương pháp DE thực hiện như sau đây. Đầu tiên, tính hiệu h và trung bình cộng l của (x, y) như sau:

$$\begin{aligned} h &= x - y, \\ l &= \left\lfloor \frac{x+y}{2} \right\rfloor, \end{aligned} \quad (1)$$

với $\lfloor \cdot \rfloor$ là phép lấy phần nguyên dưới. Nhúng bit b bằng cách mở rộng hiệu h về bên trái một bit, để thu được cặp điểm ảnh chứa tin (x', y') được tính bởi

$$\begin{aligned} h' &= 2h + b, \\ x' &= l + \left\lfloor \frac{h' + 1}{2} \right\rfloor, \\ y' &= l - \left\lfloor \frac{h'}{2} \right\rfloor. \end{aligned} \quad (2)$$

Nhận xét: Dễ dàng chứng minh được tính bảo toàn của trung bình cộng, nghĩa là

$$l' = \left\lfloor \frac{x' + y'}{2} \right\rfloor = \left\lfloor \frac{x + y}{2} \right\rfloor = l.$$

2) Khái niệm khả mở:

Cặp điểm ảnh (x, y) được gọi là khả mở (expandable) [8] nếu sau khi giấu một bit $b \in \{0, 1\}$ vào (x, y) theo các công thức (1) và (2) thì các điểm của cặp điểm ảnh chứa tin (x', y') cũng nằm trong miền giá trị điểm ảnh (tức là $x', y' \in [0, 255]$).

Nhận xét 1:

- Nếu h càng nhỏ (về giá trị tuyệt đối) thì sự sai khác giữa (x', y') và (x, y) cũng càng nhỏ, do đó (x, y) có mức độ khả mở càng cao.
- Trong phương pháp DE, nếu cặp khả mở (x, y) được sử dụng để nhúng một bit b thì từ cặp (x', y') có thể trích bit dữ liệu b và khôi phục cặp điểm ảnh gốc (x, y) như sau:

$$\begin{aligned} h' &= x' - y', \quad b = h' \bmod 2, \quad h = \left\lfloor \frac{h'}{2} \right\rfloor, \\ l &= \left\lfloor \frac{x' + y'}{2} \right\rfloor, \quad x = l + \left\lfloor \frac{h+1}{2} \right\rfloor, \quad y = l - \left\lfloor \frac{h}{2} \right\rfloor. \end{aligned} \quad (3)$$

3) Khái niệm bản đồ định vị:

Bản đồ định vị (location map) [8] là dãy bit nhị phân nhằm đánh dấu các cặp điểm khả mở. Để xây dựng bản đồ định vị, ảnh gốc được duyệt lần lượt từ trái sang phải, trên xuống dưới, khi gặp một cặp điểm khả mở, giá trị 1 được ghi vào bản đồ, còn lại là giá trị 0.

Bản đồ định vị cần sử dụng trong giai đoạn khôi phục dữ liệu và ảnh gốc, vì vậy nó cần được nén bảo toàn và nhúng vào chính các cặp khả mở. Vì vậy, khả năng nhúng của phương pháp DE được đánh giá theo công thức

$$C = \|E\| - \|MN\|, \quad (4)$$

trong đó, E là tập các cặp khả mở, MN là dãy bit nén của bản đồ, $\|\cdot\|$ biểu diễn kích thước (số phần tử) của một tập hay của một dãy bit.

2. Phương pháp dự báo

Từ (4) và nhận xét 1 dễ dàng nhận thấy, để tăng khả năng nhúng C của phương pháp DE cần tạo ra nhiều hiệu nhỏ.

Để đạt được mục tiêu này, người ta đã sử dụng các phương pháp dự báo.

Các phương pháp dự báo đầu tiên được đề xuất vào năm 2004 bởi Thodi cùng cộng sự [12] và Phiasai cùng các cộng sự [13]. Trong các phương pháp này, mỗi điểm ảnh x sẽ được dự báo bởi các điểm ảnh lân cận gọi là ngữ cảnh dự báo (prediction context) [10, 12] $y = P(x)$. Dự báo $P(x)$ được xác định dựa trên các điểm lân cận của x và càng gần x càng tốt.

Những phương pháp dự báo hay được sử dụng là dự báo hình thoi hay quả trám (Rhombus Pattern) [10], dự báo gradient (GAP: Gradient Adjusted Prediction) [4], dò biên trung vị (MED: Median Edge Detector) [12], dự báo linh hoạt trên từng vùng ảnh [1], v.v.

Sau khi xác định giá trị dự báo y của x , ta tính sai số dự báo $e = x - y$ và nhúng một bit b bằng cách mở rộng sai số dự báo để được điểm ảnh x' bởi

$$\begin{aligned} e' &= 2e + b, \\ x' &= y + e' = x + e + b. \end{aligned}$$

Vì vậy, phương pháp này còn gọi là mở rộng lỗi dự báo (PEE: Prediction Error Expansion). Trong phương pháp PEE, điểm ảnh x được gọi là khả mở nếu $x' \in [0, 255]$.

Nhận xét 2:

- Đối tượng được xem xét để nhúng tin trong phương pháp PEE là điểm ảnh, với số lượng nhiều gấp đôi số lượng cặp điểm ảnh là đối tượng được sử dụng bởi phương pháp DE.
- Sai số dự báo cho điểm ảnh thường nhỏ do giá trị dự báo gần với giá trị gốc, do đó khả năng nhúng tin của phương pháp PEE cao hơn so với phương pháp DE.

3. Phương pháp Sachnev

Phương pháp nhúng tin Sachnev [10] sử dụng ngữ cảnh dự báo hình thoi, mỗi điểm ảnh I_{ij} được dự báo theo ngữ cảnh gồm 4 điểm tạo nên một hình thoi có tâm I_{ij} (Hình 1) theo công thức sau:

$$\hat{I}_{ij} = \left\lfloor \frac{I_{i,j-1} + I_{i+1,j} + I_{i,j+1} + I_{i-1,j}}{4} \right\rfloor. \quad (5)$$

	$I_{i-1,j}$	
$I_{i,j-1}$	$I_{i,j}$	$I_{i,j+1}$
	$I_{i+1,j}$	

Hình 1. Bốn điểm ảnh tạo nên ngữ cảnh dự báo hình thoi cho điểm I_{ij} .

Bít dữ liệu b được nhúng theo phương pháp mở rộng sai số dự báo như sau:

$$\begin{aligned} e_{ij} &= I_{ij} - \widehat{I}_{ij}, \\ e'_{ij} &= 2 * e_{ij} + b, \\ I'_{ij} &= \widehat{I}_{ij} + e'_{ij} = I_{ij} + e_{ij} + b. \end{aligned} \quad (6)$$

Nếu $I'_{ij} \in [0, 255]$ thì I_{ij} được gọi là khả mở và việc nhúng tin hoàn tất. Khi đó từ I'_{ij} và $\widehat{I}_{ij}$ ($\widehat{I}_{ij}$ bất biến trong quá trình nhúng tin) có thể khôi phục bít b và ảnh gốc I_{ij} theo như sau:

$$\begin{aligned} e'_{ij} &= I'_{ij} - \widehat{I}_{ij}, \quad b = e'_{ij} \bmod 2, \\ e_{ij} &= \left\lfloor \frac{e'_{ij}}{2} \right\rfloor, \quad I_{ij} = \widehat{I}_{ij} + e_{ij}. \end{aligned} \quad (7)$$

Sachnev và cộng sự đã đưa ra một đại lượng có tính chất bất biến đối với quá trình nhúng tin, được gọi là phương sai địa phương (local variance) [10] của ngữ cảnh dự báo của I_{ij} :

$$v_{ij} = \frac{1}{4} \sum_{k=1}^4 (d_k - \bar{d})^2, \quad (8)$$

với $d_1 = |I_{(i,j-1)} - I_{(i-1,j)}|$, $d_2 = |I_{(i-1,j)} - I_{(i,j+1)}|$, $d_3 = |I_{(i,j+1)} - I_{(i+1,j)}|$, $d_4 = |I_{(i+1,j)} - I_{(i,j-1)}|$, $\bar{d} = \frac{1}{4} \sum_{k=1}^4 d_k$. Các tác giả đưa ra một nhận xét quan trọng: Nếu v_{ij} càng nhỏ thì e_{ij} càng nhỏ, dẫn đến sự sai khác giữa I'_{ij} và I_{ij} cũng càng nhỏ và khả năng $I'_{ij} \in [0, 255]$ càng cao, tức là I_{ij} càng có nhiều cơ hội rơi vào tập khả mở. Từ đó Sachnev và cộng sự đề xuất một cải tiến quan trọng: Sắp xếp các I_{ij} theo thứ tự tăng dần của phương sai địa phương v_{ij} và thực hiện việc nhúng tin vào các điểm ảnh theo thứ tự được sắp xếp. Bằng cách như vậy, hầu hết các điểm ảnh khả mở sẽ dồn lên phía trên, do đó, trong nhiều trường hợp chúng ta không cần dùng đến bản đồ định vị.

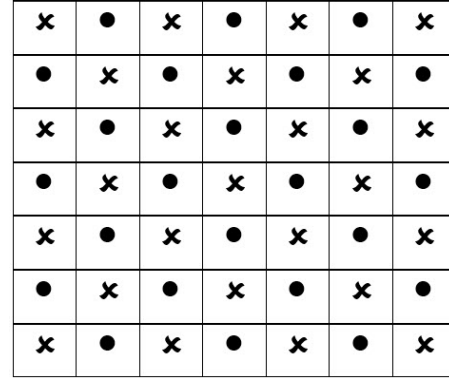
III. PHƯƠNG PHÁP ĐỀ XUẤT

Phương pháp đề xuất thực hiện việc nhúng trên các điểm ảnh có phương sai địa phương nhỏ và ngữ cảnh dự báo nằm sâu bên trong miền điểm ảnh $[0, 255]$. Chúng tôi cũng sử dụng dự báo hình thoi như trong [10]. Ảnh gốc I được chia thành hai tập điểm ảnh rời nhau, được biểu diễn bởi các dấu chấm $\bullet$ (tập chẵn) và các dấu chéo $\times$ (tập chẵn) như hình 2.

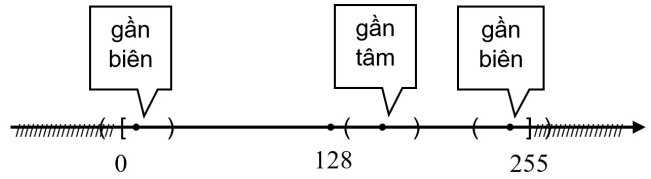
Cách phân chia điểm ảnh vào hai tập cần đảm bảo yêu cầu là hai điểm ảnh kề nhau trên cùng hàng hoặc cùng cột phải được đánh dấu khác nhau. Gọi $D(i, j)$ là dấu của điểm ảnh (i, j) . Để đạt được yêu cầu trên, có thể xác định $D(i, j)$ theo công thức

$$D(i, j) = \begin{cases} \bullet, & \text{nếu } i + j \bmod 2 = 1, \\ \times, & \text{còn lại.} \end{cases}$$

Để đơn giản, ta chỉ xét thuật toán nhúng trên tập chẵn, còn tập chẵn dùng làm ngữ cảnh dự báo.



Hình 2. Phân chia các điểm ảnh thành hai tập.



Hình 3. Độ sâu của ngữ cảnh dự báo.

	247	
245	252	253
	253	

	135	
140	120	105
	115	

(a) Không khả mở

(b) Khả mở

Hình 4. Các ví dụ minh họa vai trò độ sâu ngữ cảnh.

1. Cải tiến phương pháp sắp xếp

Trong lược đồ đề xuất, thay vì chỉ quan tâm đến phương sai địa phương như trong lược đồ Sachnev, chúng tôi còn xét xem ngữ cảnh có nằm sâu bên trong miền điểm ảnh hay không. Thật vậy, sau khi nhúng một bít vào điểm ảnh có giá trị x sẽ nhận được x' sai khác với x một giá trị $\pm \alpha$ ($\alpha \geq 0$). Nếu x càng gần tâm miền điểm ảnh, thì đoạn $[x - \alpha, x + \alpha]$ càng có nhiều khả năng nằm trong $[0, 255]$, tức là $x' \in [0, 255]$ và x khả mở (xem hình 3).

Để minh họa thêm cho vai trò của vị trí ngữ cảnh dự báo trong $[0, 255]$ đối với tính khả mở của điểm ảnh, ta xem xét ví dụ như trong hình 4.

Trường hợp 1 (hình 4(a)): điểm ảnh gốc $I_{ij} = 252$ và dự báo $\widehat{I}_{ij} = 249$, phương sai địa phương $v_{ij} = 10$, nhúng bít $b = 1$ theo (7):

$$\begin{aligned} e &= I_{ij} - \widehat{I}_{ij} = 3, \\ I'_{ij} &= I_{ij} + e + b = 256. \end{aligned}$$

Do $I_{ij} > 255$ nên điểm $I_{ij} = 252$ không khả mở mặc dù có phương sai địa phương nhỏ.

Trường hợp 2 (hình 4(b)): điểm ảnh gốc $I_{ij} = 120$ và dự báo $\hat{I}_{ij} = 123$, phương sai địa phương $v_{ij} = 106,25$, nhúng bit $b \in \{0, 1\}$ theo (7):

$$e = I_{ij} - \hat{I}_{ij} = -3, \\ I'_{ij} = I_{ij} + e + b = 117 + b.$$

Rõ ràng $I'_{ij} \in [0, 255]$ với $b \in \{0, 1\}$, nên $I_{ij} = 120$ khả mở dù có phương sai địa phương lớn. Với hai ví dụ trên, rõ ràng tính khả mở của một điểm ảnh không chỉ phụ thuộc vào phương sai của ngữ cảnh dự báo mà còn bị chi phối bởi một yếu tố khác đó là vị trí của ngữ cảnh trong đoạn $[0, 255]$. Ngữ cảnh dự báo của I_{ij} càng nằm sâu bên trong $[0, 255]$ thì cơ hội khả mở của I_{ij} càng lớn. Để đánh giá độ sâu này, chúng tôi sử dụng khoảng cách giữa tâm ngữ cảnh dự báo và tâm đoạn $[0, 255]$ (giá trị 128) là

$$d_{ij} = \left| 128 - \frac{I_{i,j-1} + I_{i+1,j} + I_{i,j+1} + I_{i-1,j}}{4} \right|, \quad (9)$$

trong đó $|\cdot|$ là phép lấy giá trị tuyệt đối của một số thực.

Chúng tôi sử dụng một giá trị kết hợp giữa khoảng cách hai tâm và phương sai địa phương bởi

$$c_{ij} = \alpha v_{ij} + d_{ij} \quad (10)$$

để thực hiện sắp xếp các điểm ảnh. Hệ số α là khác nhau đối với mỗi ảnh thử nghiệm. Gọi $F(\alpha)$ là độ lớn vùng khả mở ứng với α . Qua thử nghiệm, ta thấy $F(\alpha)$ có tính chất là $F(\alpha)$ tăng dần khi α tăng dần từ 1, đạt đến một điểm cực đại (tại $\alpha_{\max}$) rồi giảm dần (Hình 8). Dựa vào tính chất này để dàng xác định $\alpha_{\max}$ bằng phép lặp tuần tự. Xuất phát từ $\alpha = 1$, tăng dần α theo bước nhảy Δ , khi nào $F(\alpha)$ bắt đầu giảm thì có nghĩa $F(\alpha)$ đã đạt được cực đại ở α trước.

Để minh họa ý tưởng sắp xếp các điểm ảnh của tập chấm, ta xét ảnh I như trong hình 2. Đầu tiên lọc ra các vị trí (hàng, cột) của các phần tử I_{ij} và giá trị c_{ij} (của tập chấm, nhưng không xét các điểm trên biên ảnh) để tạo thành hai dãy (theo thứ tự trên xuống, trái sang phải) như hình 5. Giả sử dãy $\{c_{ij}\}$ có các giá trị như trong hình 6, thì sau khi sắp xếp $\{I_{ij}\}$ theo chiều tăng của $\{c_{ij}\}$ ta nhận được dãy $\{(i, j)\}_s$ trong hình 7. Quá trình sắp xếp không làm thay đổi vị trí các điểm ảnh của ảnh gốc I , mà chỉ nhằm tạo ra dãy $\{(i, j)\}_s$.

2. Cải thiện khả năng nhúng và chất lượng ảnh

Phương pháp Sachnev vẫn sử dụng bản đồ định vị để phân biệt các điểm ảnh khả mở và không khả mở. Do đó, khả năng nhúng cực đại của phương pháp này vẫn được tính theo công thức (4). Cái mới ở đây là bản đồ định vị, MN , được xây dựng sau khi sắp xếp các điểm ảnh theo chiều tăng của phương sai địa phương nên $\|MN\|$ nhỏ, do đó khả năng nhúng của phương pháp Sachnev được cải thiện so với các phương pháp trước đó.

Trong trường hợp độ dài của dãy bit dữ liệu D nhỏ hơn C , phương pháp Sachnev sử dụng hai giá trị ngưỡng T_n và T_p . Tập các điểm khả mở và bản đồ khi đó được xây dựng qua các ngưỡng và chúng được ký hiệu lần lượt là $E(T_n, T_p)$ và $MN(T_n, T_p)$. Khả năng nhúng cũng phụ thuộc vào ngưỡng và được xác định theo công thức

$$C(T_n, T_p) = \|E(T_n, T_p)\| - \|MN(T_n, T_p)\|.$$

Vấn đề là cần xác định các ngưỡng T_n và T_p sao cho khả năng nhúng vừa bằng độ dài dãy bit dữ liệu D đồng thời ảnh sau khi nhúng bị biến đổi ít nhất (chất lượng ảnh chứa tin cao nhất).

Trong [10], Sachnev và cộng sự sử dụng một thuật toán lặp để xác định T_n và T_p . Dễ dàng nhận thấy trong phương pháp Sachnev còn tồn tại hai vấn đề. Thứ nhất, bản đồ định vị vẫn được sử dụng để phân biệt các điểm ảnh khả mở và không khả mở, nên việc cải thiện khả năng nhúng chưa cao. Thứ hai, ngoài các điểm ảnh khả mở bị biến đổi một lượng bằng sai số dự báo để nhúng tin, hầu hết các điểm ảnh còn lại cũng bị biến đổi một giá trị bằng ngưỡng T_n hoặc T_p . Vì vậy chất lượng ảnh chứa tin còn chưa cao.

Phương pháp đề xuất khai thác các đoạn khả mở nhận được bằng cách sắp xếp theo phương pháp trong mục III-1. Để xác định vị trí của mỗi đoạn chỉ cần lưu trữ khoảng cách từ điểm đầu của đoạn đang xét đến đoạn trước và độ dài của đoạn này, cần 32 bit.

Thông thường cần dùng khoảng 4-5 đoạn, tương ứng với 128-160 bit, và tối đa là 10 đoạn, tương ứng với 320 bit thông tin phụ, ít hơn nhiều so với độ dài mã nén của bản đồ định vị. Do vậy khả năng nhúng của phương pháp đề xuất được gia tăng so với phương pháp Sachnev.

Khi độ dài của dãy bit dữ liệu D nhỏ hơn khả năng nhúng C , phương pháp đề xuất sử dụng một số đoạn đầu tiên hoặc một số đoạn dài vừa đủ để nhúng D . Các điểm ảnh ở đầu thường có sai số nhỏ, nên độ biến đổi của chúng sau khi nhúng không lớn. Ngoài ra, tất cả các điểm ảnh không sử dụng để nhúng tin sẽ được giữ nguyên (không biến đổi), nên ảnh chứa tin nhận được theo phương pháp đề xuất có chất lượng tốt hơn so với phương pháp Sachnev.

Để minh họa việc sử dụng các đoạn khả mở, ta xét ví dụ về dãy $\{(i, j)\}_s$ nhận được sau khi sắp xếp như trong hình 7. Giả sử, tính chất khả mở của các điểm ảnh tại các vị trí $\{(i, j)\}_s$ được liệt kê như trong hình 9 (K là khả mở, 0 là không khả mở). Khi đó, nếu cần nhúng 7 bit thông tin thì ta chọn hai đoạn khả mở ($T = 2$): các đoạn từ vị trí 1 đến 4 và từ vị trí 8 đến 10 trên dãy $\{(i, j)\}_s$.

Để định vị đoạn t ($t = 1, \dots, T$) ta dùng hai giá trị nguyên kc_t và dd_t , trong đó kc_t là khoảng cách đến đoạn trước $t-1$ (nếu $t = 1$ thì $kc = 1$) và dd_t là độ dài đoạn t . Trong ví dụ này, thông tin về các đoạn khả mở là $T = 2$ (chọn 2 đoạn để nhúng tin), $kc_1 = 1$, $dd_1 = 4$, $kc_2 = 4$, $dd_2 = 3$. Bấy

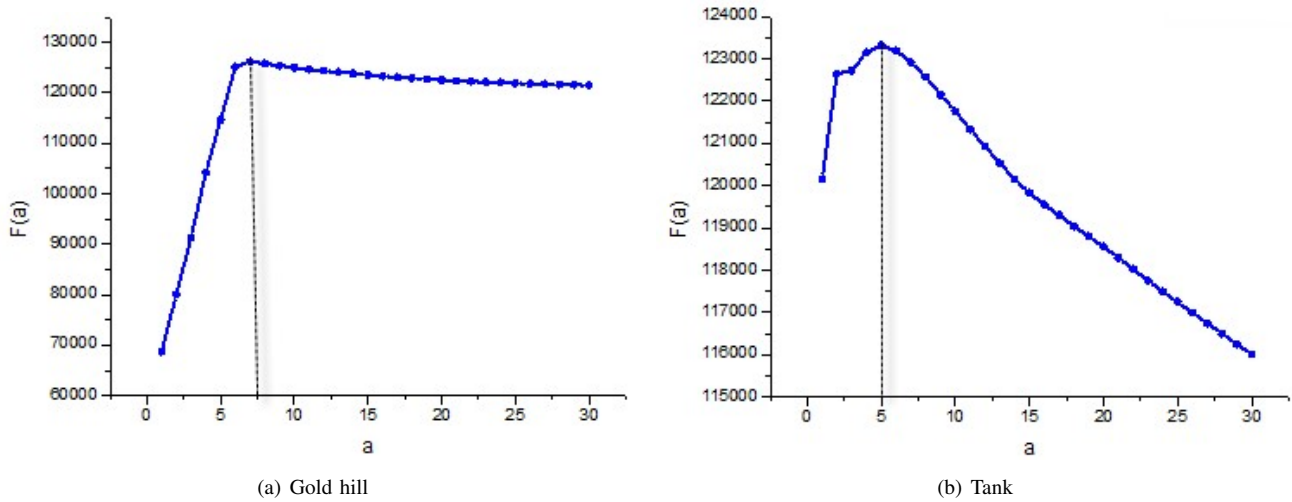
STT	1	2	3	4	5	6	7	8	9	10	11	12
$\{(i, j)\}$	(2,3)	(2,5)	(3,2)	(3,4)	(3,6)	(4,3)	(4,5)	(5,2)	(5,4)	(5,6)	(6,3)	(6,5)
$\{c_{ij}\}$	c_{23}	c_{25}	c_{32}	c_{34}	c_{36}	c_{43}	c_{45}	c_{52}	c_{54}	c_{56}	c_{63}	c_{65}

Hình 5. Dãy vị trí tập chấm $\{(i, j)\}, \{c_{ij}\}$ ban đầu.

$\{c_{ij}\}$	5.5	7	2	1	8.3	9	12	8	3	4	2	1
--------------	-----	---	---	---	-----	---	----	---	---	---	---	---

Hình 6. Dãy $\{c_{ij}\}$.

STT	1	2	3	4	5	6	7	8	9	10	11	12
$\{(i, j)\}_s$	(3,4)	(6,5)	(3,2)	(6,3)	(5,4)	(5,6)	(2,3)	(2,5)	(5,2)	(3,6)	(4,3)	(4,5)

Hình 7. Dãy $\{(i, j)\}_s$ sau khi sắp xếp.Hình 8. Đồ thị khả năng nhúng khi α biến thiên.

$\{(i, j)\}_s$	(3,4)	(6,5)	(3,2)	(6,3)	(5,4)	(5,6)	(2,3)	(2,5)	(5,2)	(3,6)	(4,3)	(4,5)
Tính chất khả mở	K	K	K	K	0	K	0	K	K	K	0	0

Hình 9. Tính khả mở của dãy $\{I(i, j)\}$ tại các vị trí $\{(i, j)\}_s$ ban đầu.

điểm ảnh trên tập chấm được dùng để nhúng tin lần lượt là (3,4), (6,5), (3,2), (6,3) của đoạn 1 và (2,5), (5,2), (3,6) của đoạn 2.

3. Thuật toán nhúng dữ liệu

Đầu vào của thuật toán nhúng dữ liệu là ảnh đa mức xám I và dãy bit dữ liệu D . Đầu ra là ảnh I' chứa D và các bit bổ trợ cần dùng trong thuật toán khôi phục.

Bước 1: Chia tập các điểm ảnh thành tập chấm ($\bullet$) và tập chéo ($\times$) (hình 2). Tập chấm được dùng để nhúng dữ

liệu còn tập chéo được sử dụng làm ngữ cảnh dự báo.

Bước 2: Tính các phương sai địa phương v_{ij} theo công thức (8), khoảng cách d_{ij} giữa tâm miền điểm ảnh với tâm ngữ cảnh theo công thức (9) và $\hat{I}_{ij}$ theo công thức (5).

Bước 3: Xác định hệ số α để đạt được đoạn khả mở đầu tiên lớn nhất theo các giá trị v_{ij} và d_{ij} bằng phương pháp lặp. Thực nghiệm chứng tỏ có thể lấy α là một giá trị nguyên trong đoạn $[2, 255]$.

Bước 4: Sau khi có α , tính giá trị tổ hợp c_{ij} theo công thức (10). Sắp xếp các điểm ảnh I_{ij} của tập chấm theo thứ

Bảng I
CẤU TRÚC THÔNG TIN BỔ TRỢ A

Ký hiệu	Ý nghĩa	Độ dài theo bit
T	Số đoạn khả mở được chọn	4
LSB	8 bit thấp của $I_{u_t v_t}$ ($t = 1, \dots, 8$)	8
size(D)	Độ dài dãy bit D	20
kc_1	$kc_1 = 1$	16
dd_1	Độ dài đoạn thứ 1	16
...		
kc_T	Khoảng cách từ đoạn T đến đoạn trước $T - 1$	16
dd_T	Độ dài đoạn thứ T	16

tự tăng của c_{ij} để nhận được dãy $\{(i, j)\}_s$ (xem mục III-1).

Bước 5: Xác định thông tin bổ trợ A.

Trước hết, chọn tám điểm ảnh, ký hiệu $I_{u_t v_t}$ ($t = 1, \dots, 8$), dùng để lưu trữ giá trị α . Các điểm này cần không tham gia quá trình dự báo cũng như quá trình nhúng tin. Sau đó, xác định số đoạn khả mở T dùng để nhúng D và A.

Thông tin bổ trợ A bao gồm:

- Bit thấp của tám điểm ảnh $I_{u_t v_t}$ ($t = 1, \dots, 8$), ký hiệu LSB;
- Độ dài dãy bit dữ liệu D , ký hiệu size(D);
- Số đoạn khả mở được chọn T ;
- Thông tin định vị của đoạn t ($t = 1, \dots, T$), được xác định bởi hai số nguyên kc_t và dd_t như mục III-2.

Cấu trúc thông tin bổ trợ A như trong bảng I, với T là giá trị nguyên nhỏ nhất thỏa mãn $dd_1 + dd_2 + \dots + dd_T \geq \text{size}(A) + \text{size}(D)$.

Ví dụ, thông thường với $T \leq 10$ thì $\text{size}(A) \leq 352$, thông tin này hoàn toàn có thể nhúng trong đoạn khả mở đầu tiên.

Bước 6: Xác định dãy bit cần nhúng $B = A + D$.

Bước 7: Nhúng lần lượt các bit của B vào T đoạn khả mở được chọn theo công thức (6).

Bước 8: Nhúng α trên tám bit thấp của các điểm ảnh $I_{u_t v_t}$ ($t = 1, \dots, 8$).

Kết quả ta nhận được ảnh I' vừa chứa D vừa chứa thông tin bổ trợ A dùng cho quá trình khôi phục.

4. Thuật toán trích tin giấu và khôi phục ảnh gốc

Thực hiện khôi phục dữ liệu D và ảnh gốc I từ ảnh chứa tin I' như sau.

Bước 1: Chia ảnh I thành tập chấm (•) và tập chéo (×) giống như trong thuật toán nhúng.

Bước 2: Xác định phương sai địa phương v_{ij} theo công thức (8), khoảng cách giữa tâm miền điểm ảnh với tâm ngữ

cảnh d_{ij} theo công thức (9) và $\hat{I}_{ij}$ theo công thức (5) cho các điểm I'_{ij} thuộc tập chấm.

Bước 3: Trích tám bit thấp của các điểm ảnh $I'_{u_t v_t}$ ($t = 1, \dots, 8$) để xác định α .

Bước 4: Sau khi có α , tính giá trị tổ hợp c_{ij} theo công thức (10) và sắp xếp các I'_{ij} của tập chấm theo thứ tự tăng dần của c_{ij} (xem mục III-1).

Bước 5: Sử dụng bốn điểm ảnh đầu của đoạn khả mở thứ nhất để trích bốn bit và khôi phục bốn điểm ảnh này theo (7). Từ bốn bit vừa trích, ta xác định được giá trị T (số đoạn khả mở).

Bước 6: Sử dụng $28 + 32T$ điểm ảnh tiếp theo của đoạn khả mở thứ nhất để khôi phục phần còn lại của A và các điểm ảnh gốc tương ứng (theo (7)).

Bước 7: Khôi phục size(D) bit dữ liệu và các điểm ảnh tương ứng từ phần còn lại của đoạn khả mở thứ nhất và các đoạn khả mở tiếp theo (cũng theo (7)).

Bước 8: Chèn giá trị LSB (có trong A) vào các bit thấp của các điểm ảnh $I'_{u_t v_t}$ ($t = 1, \dots, 8$) để khôi phục $I_{u_t v_t}$ ($t = 1, \dots, 8$).

Đến đây, ta trích được dãy bit dữ liệu D và khôi phục toàn bộ ảnh gốc I .

5. Nhúng tin trên toàn ảnh

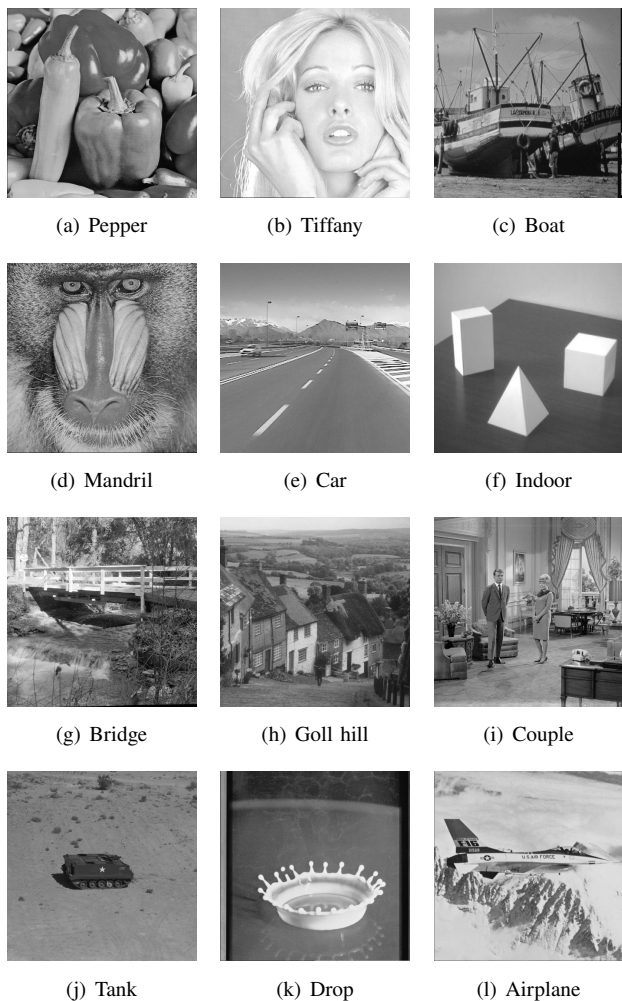
Phần trên, chúng tôi đã trình bày việc nhúng dữ liệu trên tập chấm và dùng tập chéo để làm ngữ cảnh dự báo. Có thể nâng khả năng nhúng gấp đôi bằng cách: sau khi nhúng dữ liệu trên tập chấm, ta tiếp tục thực hiện nhúng trên tập chéo. Lúc đó tập chấm (đã biến đổi) sẽ là ngữ cảnh dự báo cho tập chéo. Khi thực hiện trích tin và khôi phục ảnh gốc, ta tiến hành theo thứ tự ngược lại, đó là trích tin và khôi phục các điểm ảnh của tập chéo, sau đó sẽ thực hiện trích tin và khôi phục các điểm ảnh thuộc tập chấm.

IV. THỬ NGHIỆM VÀ SO SÁNH

Để minh họa các kết quả phân tích bên trên, chúng tôi đã tiến hành thử nghiệm trên bộ ảnh mẫu trong [14] với nhiều loại ảnh khác nhau có cùng kích cỡ 512×512 (xem hình 10), bao gồm ảnh thông thường (common images) như Pepper, ảnh đan xen (texture images) như Mandril, ảnh sáng màu (high-tone images) như Tiffany, ảnh chứa nhiều vùng phẳng (flat regions) như Car, ảnh với các bộ phận đan xen và độ sáng không đồng đều như Boat và ảnh khối hình học như Indoor, v.v. Chương trình viết cho MATLAB R2012a và chạy trên máy tính Lenovo Ideapad S410p.

1. So sánh khả năng nhúng tin khi dùng đoạn khả mở đầu tiên với phương pháp Sachnev

Đoạn khả mở đầu tiên là đoạn quan trọng và phải đủ lớn để lưu trữ toàn bộ thông tin phụ. Bảng II cho thấy phương



Hình 10. Một số ảnh trong thử nghiệm.

pháp đề xuất cho đoạn khả mở đầu tiên cao hơn hẳn phương pháp Sachnev (gấp khoảng hai lần), điều đó cho thấy vai trò của độ sâu ngữ cảnh trong việc dồn các điểm khả mở về phía trước.

2. So sánh với các phương pháp gần đây

Để minh họa ưu điểm của phương pháp đề xuất, chúng tôi chọn hai phương pháp giấu tin thuận nghịch gần đây để so sánh, đó là phương pháp Qu (năm 2015) [11] và phương pháp Kumar (năm 2016) [2].

1) So sánh khả năng nhúng:

Với chất lượng ảnh chứa tin theo hệ số PSNR lớn hơn hoặc bằng 30 (mức tối thiểu chấp nhận được của chất lượng ảnh theo [15, tr. 6]), phương pháp đề xuất có khả năng nhúng cao hơn cả hai phương pháp Kumar và Qu như được chỉ ra ở bảng III.

2) So sánh về chất lượng ảnh:

Với cùng một số bit dữ liệu được nhúng như nhau, phương pháp đề xuất có hệ số PSNR gần tương đương

Bảng II
SO SÁNH ĐOẠN KHẢ MỞ ĐẦU TIÊN
TIỀN VỚI PHƯƠNG PHÁP SACHNEV

Ảnh thử nghiệm	Đoạn khả mở đầu tiên	
	Sachnev	Đề xuất
Car	23236	26949
Pepper	11365	22003
Tiffany	277	1972
Boat	80482	81450
Mandril	1419	5089
Indoor	1304	90468
Bridge	215	129541
Goll hill	118510	126186
Couple	1250	86470
Tank	100661	123312
Drop	126584	129541
Airplane	128404	129342
Tổng	593707	952323

Bảng III
SO SÁNH KHẢ NĂNG NHÚNG TỐI ĐA (THEO BÍT)

Ảnh thử nghiệm	Kumar (PSNR $\approx$ 30)	Qu (khối 2×2)	Đề xuất
Car	1780	16462	29523
Pepper	7030	34130	31206
Tiffany	2040	11285	29951
Boat	6850	35585	96962
Mandril	6450	22025	93676
Indoor	5450	81231	95585
Bridge	9000	68576	129541
Goll hill	13000	32060	130036
Couple	8000	42180	86470
Tank	7800	72954	128755
Drop	7000	68576	129541
Airplane	8000	71539	130049
Tổng	82400	556603	1111295

với phương pháp Qu và cao hơn nhiều so với phương pháp Kumar (xem bảng IV).

V. KẾT LUẬN

Phương pháp giấu tin thuận nghịch được đề xuất dựa trên các ý tưởng sau. Đầu tiên, sắp xếp các điểm ảnh theo chiều tăng của phương sai địa phương kết hợp với khoảng cách giữa tâm miền điểm ảnh với tâm ngữ cảnh dự báo, để dồn hầu hết các điểm ảnh khả mở lên phía trên. Sau đó khai thác các đoạn khả mở để nhúng tin. Thay cho việc sử dụng bản đồ định vị nén (có độ dài khá lớn), mỗi đoạn khả mở được xác định bởi hai số nguyên có độ dài 16 bit, do đó khả năng nhúng và chất lượng ảnh được cải thiện so với một số phương pháp gần đây.

Bảng IV
SO SÁNH CHẤT LƯỢNG ẢNH (THEO PSNR)

Ảnh thử nghiệm	Kumar	Qu	Đề xuất
Car	18,8639	58,1079	44,0582
Pepper	33,2160	63,3236	55,2678
Tiffany	38,0515	68,8400	64,7945
Boat	32,2601	64,7838	70,3490
Mandrill	21,9831	59,7622	45,9813
Indoor	36,1376	70,4338	70,2982
Bridge	28,9416	61,2098	58,3108
Goll hill	29,5007	59,7402	52,0942
Couple	29,4136	60,2730	53,5863
Tank	29,4923	61,8325	53,8388
Drop	30,0188	62,1474	59,2189
Airplane	29,5731	62,1866	59,5129

TÀI LIỆU THAM KHẢO

- [1] I.-C. Dragoi and D. Coltuc, "Local-prediction-based difference expansion reversible watermarking," *IEEE Transactions on Image Processing*, vol. 23, no. 4, pp. 1779–1790, 2014.
- [2] M. Kumar and S. Agrawal, "Reversible data hiding based on prediction error expansion using adjacent pixels," *Security and Communication Networks*, vol. 9, pp. 3703–3712, 2016.
- [3] B. Macq, "Lossless multiresolution transform for image authenticating watermarking," in *Proceedings of the 10th European Signal Processing Conference*, 2000, pp. 1–4.
- [4] X. Wu and N. Memon, "Context-based, adaptive, lossless image coding," *IEEE Transactions on Communications*, vol. 45, no. 4, pp. 437–444, 1997.
- [5] J. Fridrich, M. Goljan, and R. Du, "Invertible authentication," in *Proceedings of the Security and Watermarking of Multimedia contents III*, vol. 4314, 2001, pp. 197–209.
- [6] K. Sao Nguyen, Q. H. Le, and V. A. Pham, "A new reversible watermarking method based on histogram shifting," *Applied Mathematical Sciences*, vol. 11, pp. 445–460, 2017.
- [7] J.-D. Lee, Y.-H. Chiou, and J.-M. Guo, "Reversible data hiding based on histogram modification of SMVQ indices," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 4, pp. 638–648, 2010.
- [8] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Transactions on Circuits and System for Video Technology*, vol. 13, no. 8, pp. 890–896, 2003.
- [9] D. M. Thodi and J. J. Rodriguez, "Expansion embedding techniques for reversible watermarking," *IEEE Transactions on Image Processing*, vol. 16, no. 3, pp. 721–730, 2007.
- [10] V. Sachnev, H. J. Kim, J. Nam, S. Suresh, and Y. Q. Shi, "Reversible watermarking algorithm using sorting and prediction," *IEEE Transactions on Circuits and System for Video Technology*, vol. 19, no. 7, pp. 989–999, 2009.
- [11] X. Qu and H. J. Kim, "Pixel-based pixel value ordering predictor for high-fidelity reversible data hiding," *Signal Processing*, vol. 111, pp. 249–260, 2015.
- [12] D. M. Thodi and J. J. Rodriguez, "Reversible watermarking by prediction-error expansion," in *Proceedings of the 6th*

IEEE Southwest Symposium on Image Analysis and Interpretation, 2004, pp. 21–25.

- [13] T. Phiasai, P. Kumhom, and K. Chamnongthai, "A digital image watermarking technique using prediction method and weber ratio," in *Proceedings of the IEEE International Symposium on Communications and Information Technology (ISCIT)*, 2004, pp. 314–317.
- [14] "Images data," <http://decsai.ugr.es/cvg/dbimagenes> and <http://sipi.usc.edu/databas>, 2017.
- [15] D. Taubman and M. Marcellin, *JPEG2000 Image Compression Fundamentals, Standards and Practice*. Springer Science & Business Media, 2012, vol. 642.



phương tiện, giấu tin và thủy vân.

Nguyễn Kim Sao sinh năm 1979 tại Thái Nguyên. Tác giả tốt nghiệp Đại học Sư phạm Hà Nội năm 2001 và nhận bằng Thạc sĩ tại Trường Đại học Bách khoa Hà Nội năm 2007. Hiện nay, tác giả đang giảng dạy tại Khoa Công nghệ Thông tin, Trường Đại học Giao thông Vận tải. Lĩnh vực quan tâm nghiên cứu của tác giả là truyền thông đa



học Công nghiệp Hà Nội. Lĩnh vực quan tâm nghiên cứu của ông là an toàn thông tin, trí tuệ nhân tạo, công nghệ đa phương tiện và dữ liệu lớn.

Đỗ Văn Tuấn sinh năm 1975 tại Hải Dương. Ông nhận bằng kỹ sư tại Học viện Kỹ thuật Quân sự, bằng thạc sĩ tại Trường Đại học Công nghệ, Đại học Quốc gia Hà Nội và bằng tiến sĩ tại Trường Đại học Bách khoa Hà Nội vào các năm 2000, 2007 và 2015. Hiện nay, ông đang giảng dạy tại Khoa Công nghệ Thông tin, Trường Đại học Công nghiệp Hà Nội. Lĩnh vực quan tâm nghiên cứu của ông là an toàn thông tin, trí tuệ nhân tạo, công nghệ đa phương tiện và dữ liệu lớn.



lý ảnh, an toàn thông tin và phân tích dữ liệu.

Phạm Văn Ất sinh năm 1945 tại Hà Nội. Ông tốt nghiệp đại học năm 1967 và nhận bằng tiến sĩ năm 1980 tại Trường Đại học Tổng hợp Hà Nội. Năm 1984, ông nhận học hàm PGS. Hiện nay, ông đang giảng dạy tại Khoa Công nghệ Thông tin, Trường Đại học Giao thông Vận tải. Lĩnh vực quan tâm nghiên cứu của ông là lý thuyết ma trận, xử