

BỘ GIÁO DỤC VÀ ĐÀO TẠO  
ĐẠI HỌC QUỐC GIA HÀ NỘI  
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

Nguyễn Kim Sao

PHÁT TRIỂN MỘT SỐ PHƯƠNG PHÁP  
GIẤU TIN VÀ THỦY VÂN THUẬN  
NGỊCH ỨNG DỤNG TRONG XÁC  
THỰC BẢN QUYỀN VÀ BẢO MẬT DỮ  
LIỆU ĐA PHƯƠNG TIỆN

LUẬN ÁN TIẾN SỸ CÔNG NGHỆ THÔNG  
TIN

Hà Nội - 2019

**BỘ GIÁO DỤC VÀ ĐÀO TẠO  
ĐẠI HỌC QUỐC GIA HÀ NỘI  
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ**

**Nguyễn Kim Sao**

**PHÁT TRIỂN MỘT SỐ PHƯƠNG PHÁP  
GIẤU TIN VÀ THỦY VÂN THUẬN  
NGỊCH ỨNG DỤNG TRONG XÁC  
THỰC BẢN QUYỀN VÀ BẢO MẬT DỮ  
LIỆU ĐA PHƯƠNG TIỆN**

Chuyên ngành: Hệ thống thông tin

Mã số: 9480104.01

**NGƯỜI HƯỚNG DẪN KHOA HỌC:**

1. PGS. TS Phạm Văn Ất
2. PGS. TS Nguyễn Ngọc Hóa

**Hà Nội - 2019**

## MỤC LỤC

<b>MỤC LỤC</b> . . . . .	i
<b>MỞ ĐẦU</b> . . . . .	1
<b>CHƯƠNG 1. CÁC KHÁI NIỆM VÀ KIẾN THỨC CƠ SỞ</b>	<b>5</b>
1.1 Một số vấn đề về giấu tin thuận nghịch .	5
1.2 Phương pháp dịch chuyển histogram (HS) . . . . .	6
1.3 Phương pháp mở rộng hiệu . . . . .	9
<b>CHƯƠNG 2. VẤN ĐỀ TÍCH HỢP VÀ DỊCH CHUYỂN HISTOGRAM TRÊN CÁC ĐOẠN CON</b>	<b>12</b>
2.1 Tích hợp thông tin phụ trong dịch chuyển histogram . . . . .	12
2.2 Giấu tin thuận nghịch sử dụng dịch chuyển histogram trên các dãy con . . . . .	14
2.3 Phương pháp MED-SUB . . . . .	14
2.4 Cải tiến phương pháp Qu (IQ) . . . . .	16
<b>CHƯƠNG 3. THU NHỎ BẢN ĐỒ ĐỊNH VỊ TRONG PHƯƠNG PHÁP MỞ RỘNG HIỆU TRÊN MIỀN SAI SỐ DỰ BÁO</b>	<b>18</b>
3.1 Giấu tin thuận nghịch dựa trên sắp xếp sai số dự báo theo phương sai và độ lệch tâm - phương án 1 . . . . .	18

3.2	Giấu tin thuận nghịch dựa trên sắp xếp sai số dự báo theo phương sai và độ lệch tâm - Phương án 2 . . . . .	19
-----	---	----

<b>CHƯƠNG 4. GIẤU TIN TRÊN CÁC ĐIỂM ẢNH LỚN NHẤT VÀ NHỎ NHẤT CỦA MỖI KHỐI ẢNH BẰNG PVO</b>	<b>20</b>
--	-----------

4.1	Giấu tin trên các điểm ảnh lớn nhất và nhỏ nhất của mỗi khối ảnh . . . . .	20
-----	--	----

<b>KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN</b>	<b>23</b>
-------------------------------------	-----------

<b>CÁC CÔNG TRÌNH KHOA HỌC ĐÃ CÔNG BỐ</b>	<b>25</b>
---	-----------

## MỞ ĐẦU

Giấu tin là kỹ thuật nhúng một dữ liệu vào một sản phẩm ảnh số (hoặc âm thanh, video, văn bản, dữ liệu) nhằm truyền thông tin hoặc bảo vệ sản phẩm đó.

Giấu tin (data hiding) được chia thành hai hướng nghiên cứu chính: giấu tin mật (steganography) và thủy vân (watermarking) (một số tài liệu phân loại giấu tin thành giấu tin mật, thủy vân và giấu tin thuận nghịch).

Giấu tin mật chú trọng tin giấu, các tác động đều được xem xét để đảm bảo tin giấu không bị phát hiện hoặc sai lệch. Thủy vân lại chú trọng hơn đến sản phẩm, tính bền vững sẽ được dùng trong bảo vệ bản quyền sản phẩm, ngược lại tính dễ vỡ lại được dùng để xác thực tính toàn vẹn hay phát hiện giả mạo.

Một số các ứng dụng trong y tế, quân đội, luật pháp, giáo dục, . . . việc khôi phục lại ảnh gốc (sau khi nhúng thủy vân) để tiếp tục sử dụng là nhu cầu bắt buộc. Trong các trường hợp như vậy, thường phải sử dụng kỹ thuật giấu tin thuận nghịch (Reversible Data Hiding) hay còn gọi là giấu tin bảo toàn (lossless data hiding). Giấu tin thuận nghịch là kỹ thuật nhúng tin mà sau khi tách thông tin nhúng ta khôi phục được ảnh gốc ban đầu.

Thuật toán giấu tin thuận nghịch đầu tiên được Barton đề xuất vào năm 1997. Ông đề xuất nhúng thông tin xác thực vào sản phẩm số, sau khi trích xuất thông tin xác thực, người nhận có thể khôi phục được sản phẩm số ban đầu.

**Thủy vân thuận nghịch dựa trên phép biến đổi modulo** được Honsinger và cộng sự đưa ra vào

năm 2001. Phương pháp Modulo thực hiện nhúng thủy vân bằng phương pháp cộng modulo 256 (256 là giá trị tối đa có thể được cho ảnh đa mức xám 8 bit).

**Phương pháp xác thực thuận nghịch dựa trên nén bảo toàn** được Fridrich và cộng sự đề xuất. Ý tưởng của lược đồ này là tạo ra một không gian trống bằng cách nén một mặt phẳng bit của ảnh gốc, sau đó sử dụng không gian trống tạo được để nhúng dữ liệu.

**Phương pháp giấu tin dựa trên lượng tử hóa** là một sự mở rộng LSB (Generalized-LSB) và ứng dụng nó trong giấu tin thuận nghịch. Ý tưởng của phương pháp này là lượng tử hóa các điểm ảnh.

**Nhúng tin thuận nghịch trên ảnh Jpeg** hầu hết sử dụng các hệ số DCT lượng tử, bảng lượng tử và bảng mã Huffman, đặc biệt, các hệ số DCT lượng tử để thực hiện việc giấu tin thuận nghịch. Ý tưởng chung của các phương pháp là thực hiện các phép biến đổi thuận nghịch trên ba đại lượng nêu trên.

**Phương pháp mở rộng hiệu** do Jun Tian đề xuất là một trong những phương pháp giấu tin thuận nghịch đáng được quan tâm nhất. Ý tưởng của phương pháp này là nhúng một bit trên hiệu của một cặp hai điểm ảnh kề nhau dựa trên các phép biến đổi Wavelet nguyên.

**Phương pháp mở rộng sai số dự báo** (PEE-Prediction Error Expansion) là một hướng phát triển tiềm năng khác dựa trên nhận xét: nếu hiệu càng nhỏ thì khả năng để  $x$ ,  $y$  khả mở càng tăng. Vì vậy, làm sao có được các hiệu càng nhỏ càng tốt. Trên ý tưởng này, người ta đã phát triển các phương pháp dự báo.

**Dịch chuyển histogram** đề xuất như sau: trước hết, xây dựng histogram của ảnh gốc. Chọn một điểm

$a$  sao cho histogram của  $a$  lớn nhất và một điểm  $z$  sao cho histogram  $z$  nhỏ nhất. ( $a$  thường gọi là peakpoint và  $z$  gọi là zeropoint). Dịch chuyển các điểm lớn hơn  $a$  về bên phải 1 đơn vị nếu  $a < z$  hoặc về bên trái nếu  $a > z$ . Để đơn giản trong trình bày, giả sử  $a < z$ . Bằng cách như vậy,  $a + 1$  trở thành điểm trống. Nhúng dữ liệu vào điểm  $a$  như sau: Duyệt các điểm ảnh từ trái sang phải, trên xuống dưới. Nếu gặp một điểm có giá trị bằng  $a$ , sẽ giữ nguyên nếu bit cần nhúng là 0 và tăng 1 đơn vị nếu bit cần nhúng là 1. Trong phương pháp này, giá trị mỗi điểm ảnh tăng hoặc giảm nhiều nhất là một đơn vị, do đó độ biến đổi ảnh thấp tức là chất lượng ảnh chứa tin cao.

**Phương pháp giấu tin thuận nghịch dựa trên sắp xếp giá trị điểm ảnh (PVO - Pixel Value Ordering).** Ảnh được chia thành các khối, sau đó các khối được sắp xếp theo chiều tăng dần. Khi đó, một bit dữ liệu  $b$  được nhúng vào điểm ảnh có giá trị lớn nhất hoặc các giá trị lớn nhất hoặc nhỏ nhất.

### **Bố cục của luận án:**

Luận án được chia thành 4 chương:

Chương 1: Các khái niệm và kiến thức cơ sở. Chương này trình bày các khái niệm về giấu tin, các phân loại giấu tin và các ứng dụng của giấu tin. Bên cạnh đó, chương này cũng trình bày các khái niệm về giấu tin thuận nghịch, các thuật toán được sử dụng trong thủy văn thuận nghịch, các yếu tố đánh giá một lược đồ thủy văn thuận nghịch.

Chương 2: Vấn đề tích hợp và dịch chuyển histogram trên các đoạn con. Nội dung chính của chương trình bày các lược đồ thủy văn thuận nghịch liên quan đến

histogram. Các đề xuất lược đồ thủy vân mới dựa trên phép biến đổi histogram.

Chương 3: Thu nhỏ bản đồ định vị trong phương pháp mở rộng hiệu trên miền sai số dự báo. Chương này trình bày về các lược đồ thủy vân thuận nghịch liên quan, cũng như đề xuất lược đồ thủy vân mới dựa trên phép mở rộng hiệu.

Chương 4: Giấu tin trên các điểm ảnh lớn nhất và nhỏ nhất bằng PVO. Chương này trình bày về các phương pháp giấu tin thuận nghịch dựa trên dự báo sắp xếp giá trị điểm ảnh, là một phương pháp dự báo tiên tiến đang được quan tâm hiện nay. Chương cũng trình bày một phương pháp đề xuất liên quan đến cách thức dự báo này.



## CHƯƠNG 1.

### CÁC KHÁI NIỆM VÀ KIẾN THỨC CƠ SỞ

Chương này trình bày tổng quan về giấu tin thuận nghịch, các kỹ thuật thường được sử dụng trong giấu tin thuận nghịch, các phương pháp đánh giá một lược đồ giấu tin thuận nghịch cũng như những thách thức mà giấu tin thuận nghịch phải đối mặt.

#### 1.1. Một số vấn đề về giấu tin thuận nghịch

##### *Giấu tin thuận nghịch*

Đối với giấu tin truyền thống, sản phẩm sau khi trích rút dữ liệu sẽ bị biến dạng nên không thể khôi phục về trạng thái ban đầu. Trong một số lĩnh vực ứng dụng như quân đội, y tế, giáo dục, ..., việc khôi phục sản phẩm gốc ban đầu là điều bắt buộc. Để giải quyết điều này, giấu tin thuận nghịch còn được gọi là giấu tin bảo toàn được đề xuất để phục hồi chính xác cả sản phẩm gốc và dữ liệu nhúng. Các thuật toán chính dùng trong giấu tin thuận nghịch đó là mở rộng hiệu, dịch chuyển histogram và dự báo.

##### *Các yếu tố đánh giá chất lượng một lược đồ giấu tin thuận nghịch*

- Khả năng nhúng
- Đánh giá chất lượng ảnh
- Độ phức tạp

## *Những thách thức trong xây dựng lược đồ giấu tin thuận nghịch*

Tăng khả năng nhúng đồng thời cũng tăng chất lượng ảnh là một trong những thách thức đối với thủy vân thuận nghịch, khi tăng khả năng nhúng, chất lượng ảnh thông thường cũng kém đi. Bên cạnh đó, vấn đề thông tin phụ, bản đồ định vị cũng là một khó khăn cho các lược đồ thủy vân. Nếu thông tin này quá lớn, sẽ không còn nhiều không gian cho nhúng tin giấu.

### **1.2. Phương pháp dịch chuyển histogram (HS)**

Một ảnh đa cấp xám  $I$  kích cỡ  $M \times N$  có thể xem như một ma trận cấp  $M \times N$  ( $M$  hàng,  $N$  cột) gồm các phần tử  $I(i, j)$  thuộc  $D$ . Nhiều khi chỉ cần xét một miền con  $J$  nào đó của  $I$ , và ký hiệu  $P(J)$  là tập cặp chỉ số  $(i, j)$  thuộc  $J$ . Khi đó:

$$P(I) = \{(i, j) | 1 \leq i \leq M, 1 \leq j \leq N\},$$

$$P(J) = \{(i, j) | (i, j) \in J\}.$$

Gọi  $X = (x_1, x_2, \dots, x_K)$  là một dãy số nguyên cho trước, histogram của  $X$  là một hàm, ký hiệu là  $h$ , được định nghĩa như sau:

$$h(x) = \#\Omega\{1 \leq i \leq K | x_i = x\}, \forall x \in Z,$$

với  $\#\Omega$  là số phần tử của tập  $\Omega$  và  $Z$  là tập số nguyên. Nói cách khác,  $h(x)$  là số lần mà  $x$  xuất hiện (tần số) trong  $X$ .

### ***Cặp histogram***

Hai giá trị  $a, b$  ( $b = a + 1$  hoặc  $a - 1$ ) liên tiếp trên miền  $P$  được gọi là một cặp histogram nếu:

$$h(a) > 0, h(b) = 0$$

Dưới đây  $a$  và  $h(a)$  được gọi là đỉnh và chiều cao của cặp  $(a, b)$ . Mỗi điểm ảnh  $(i, j) \in P(I)$  có giá trị  $I(i, j) = a$  có thể nhúng được một bit  $w$  theo công thức:

$$x'_i = \begin{cases} a, & \text{nếu } w = 0 \\ b, & \text{nếu } w = 1 \end{cases}$$

Khi đó, thuật toán khôi phục  $w$  và  $I(i, j)$  từ  $I'(i, j)$  đơn giản như sau:

$$I(i, j) = a,$$

$$w = \begin{cases} 0, & \text{nếu } I'(i, j) = a \\ 1, & \text{nếu } I'(i, j) = b \end{cases}$$

### ***Cặp giá trị (peak, zero)***

Giá trị *peak* là giá trị điểm ảnh có histogram lớn nhất và *zero* là giá trị điểm ảnh có histogram nhỏ nhất, thông thường *zero* là giá trị điểm ảnh có histogram bằng 0:

$$peak = \{x | h(x) = \max\{h(x_i), i = 1, \dots, 255\}\}$$

$$zero = \{x | h(x) = \min\{h(x_i), i = 1, \dots, 255\}\}$$

### ***Dịch chuyển histogram***

Giả sử điểm ảnh *peak* có  $h(peak) > 0$ . Để tạo cặp histogram  $(peak, peak - 1)$  có thể sử dụng kỹ thuật dịch chuyển histogram (HS) như sau: Đầu tiên tìm điểm

$zeroL < peak$  có  $h(zeroL) = 0$ , sau đó HS trên đoạn  $[zeroL+1, peak-1]$  được dịch chuyển sang trái như sau:

$$I'(i, j) = \begin{cases} I(i, j) - 1, & \text{nếu } I(i, j) \in [zeroL + 1; peak - 1] \\ I(i, j), & \text{nếu khác} \end{cases}$$

Tương tự để tạo cặp histogram  $(peak, peak + 1)$ .

### ***Dịch chuyển histogram trên sai số dự báo***

Mỗi điểm ảnh  $x_i$  sẽ được dự báo theo một phương pháp dự báo để xác định  $\hat{x}_i$ , sau đó dãy sai số dự báo giữa điểm ảnh gốc và điểm ảnh dự báo  $E = \{e_i | e_i = x_i - \hat{x}_i\}$  được thiết lập. Dựa trên histogram của  $E$ , xác định  $e_{peak}$  và  $e_{zero}$ . Phương pháp nhúng tin và dịch chuyển trên  $E$  tương tự như trên giá trị điểm ảnh. Xác định điểm ảnh chứa tin theo công thức  $x'_i = e + \hat{x}_i$ .

Đối với phương pháp dự báo, giá trị dự báo của  $x_i$  trên ảnh gốc cũng chính là giá trị dự báo của  $x'_i$  trên ảnh nhúng tin. Đó là yếu tố quan trọng để có thể khôi phục được ảnh gốc trong giấu tin thuận nghịch.

### ***Thuật tục nhúng và trích dữ liệu bằng phương pháp HS***

Từ ảnh gốc có được dãy  $X$ , xây dựng biểu đồ histogram cho  $X$ . Thuật toán nhúng ở đây được trình bày dựa trên việc lựa chọn hai cặp giá trị  $peak, zero$  bên trái gọi là  $LPP, LZP$  và bên phải là  $RPP, RZP$  của biểu đồ histogram.

Với các cặp  $LPP, LZP, RPP, RZP$ , thực hiện việc dịch chuyển như được trình bày trong 1.2 để tạo các cặp histogram  $LPP, LPP - 1$ .

Sau đó có thể nhúng  $C$  bit (với  $C = h(LPP) + h(RPP)$ ) ở hầu hết các phần tử  $x_i$  có giá trị bằng  $LPP$  hoặc  $RPP$  như dưới đây. Duyệt  $X$  từ trái sang phải, khi tìm thấy  $x_i \in \{LPP, RPP\}$  thì  $x_i$  được thay đổi thành  $x'_i$  để nhúng 1 bit  $b$  theo công thức:

$$x'_i = \begin{cases} LPP, & \text{nếu } x_i = LPP \text{ và } b = 0 \\ LPP - 1, & \text{nếu } x_i = LPP \text{ và } b = 1 \\ RPP, & \text{nếu } x_i = RPP \text{ và } b = 0 \\ RPP + 1, & \text{nếu } x_i = RPP \text{ và } b = 1. \end{cases}$$

Do đó, khả năng nhúng tối đa của phương pháp là  $C = h(LPP) + h(RPP)$ .

Để trích xuất được  $B$  và khôi phục  $X$  từ  $X'$ , chỉ cần nghịch đảo tiến trình nhúng. Cụ thể là, trước tiên duyệt  $X'$  để trích  $B$  và khôi phục các phần tử  $x_i$  có giá trị bằng  $LPP$  hoặc  $RPP$ . Sau đó chúng ta khôi phục các phần tử  $x_i$  thuộc  $[LPP + 1, LPP - 1]$  và  $[RPP + 1, RPP - 1]$  bằng cách dịch chuyển histogram theo hướng ngược lại trong mục 1.2.

Phương pháp trên có thể được xem xét như là lược đồ tổng quát cho phương pháp HS. Các phương pháp khác nhau chủ yếu được phân biệt về cách xây dựng chuỗi số nguyên  $X$  từ ảnh gốc.

Cuối cùng, Lưu ý rằng có thể chọn hai giá trị không rộng tùy ý, Gọi  $LSP$  và  $RSP$  (điểm lựa chọn trái và phải) để tương ứng thay thế  $LPP$  và  $RPP$ . khi đó, khả năng nhúng tối đa là  $h(LSP) + h(RSP)$ .

### 1.3. Phương pháp mở rộng hiệu

#### 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. Tính hiệu  $h$  và trung bình cộng  $l$ :

$$h = x - y, \quad l = \left\lfloor \frac{x + y}{2} \right\rfloor$$

(với  $\lfloor a \rfloor$  là phần nguyên dưới của  $a$ )

Nhúng bít  $b$  bằng cách mở rộng hiệu  $h$  về bên trái một bít, được cặp điểm ảnh chứa tin  $(x', y')$ :

$$h' = 2h + b, \quad x' = l + \left\lfloor \frac{h' + 1}{2} \right\rfloor, \quad y' = l - \left\lfloor \frac{h' + 1}{2} \right\rfloor$$

Trích tin và khôi phục cặp điểm ảnh gốc: Trong phương pháp DE, mỗi cặp khả mở được sử dụng để nhúng một bít và nếu  $(x, y)$  khả mở, thì từ cặp  $(x', y')$  có thể trích bít dữ liệu  $b$  và khôi phục cặp điểm ảnh gốc  $(x, y)$  như sau:

$$h' = x' - y', \quad b = h' \bmod 2, \quad h = \left\lfloor \frac{h'}{2} \right\rfloor, \\ l = \left\lfloor \frac{x' + y'}{2} \right\rfloor, \quad x = l + \left\lfloor \frac{h + 1}{2} \right\rfloor, \quad y = l - \left\lfloor \frac{h}{2} \right\rfloor.$$

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

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

### **Phương pháp mở rộng sai số dự báo PEE (Prediction Error Expansion)**

Không giống như DE, phương pháp PEE khai thác mối tương quan địa phương của các vùng lân cận, do đó hiệu suất cũng tốt hơn. Thay vì sử dụng hiệu để nhúng tin như trong DE, PEE sử dụng sai số giữa điểm ảnh và dự báo của điểm ảnh đó.

Với mỗi điểm ảnh  $x$  có thể có một giá trị dự báo  $\hat{x}$ , sai số dự báo  $e = x - \hat{x}$ . Nhúng bít  $b$  vào sai số dự báo

$e$  được thực hiện như sau:

$$e'_i = 2e + b;$$

và giá trị điểm ảnh chứa tin là:

$$x' = \hat{x} + e' = x + 2e + b.$$

Các phương pháp dự báo thường được sử dụng đó là MED, dự báo hình thoi hay gradient. Sai số dự báo được mở rộng giống như phương pháp của DE. Đối với DE, hai điểm ảnh mới có khả năng nhúng một bit, còn với PEE, mỗi điểm ảnh có thể nhúng một bit, do đó, khả năng nhúng tin cao hơn.

## CHƯƠNG 2.

### VẤN ĐỀ TÍCH HỢP VÀ DỊCH CHUYỂN HISTOGRAM TRÊN CÁC ĐOẠN CON

Chương này trình bày ba đề xuất mới. Trong đề xuất 1 đưa ra một giải pháp đơn giản nhưng hiệu quả để tích hợp các thông tin cần cho quá trình khôi phục vào ảnh giấu tin, bằng cách chia ảnh gốc làm hai phần, một phần nhỏ chứa tin phụ còn phần lớn hơn dùng để nhúng tin bằng dịch chuyển histogram. Trong đề xuất 2 trình bày cách chia dãy sai số dự báo thành các đoạn con tương đối phẳng nhờ dùng ngưỡng cảnh dự báo, sau đó thực hiện dịch chuyển histogram trên các dãy con này. Đề xuất 3 là một sự kết hợp giữa dịch chuyển histogram và phương pháp Qu bằng cách chia dãy sai số dự báo thành hai phần nhờ dùng ngưỡng cảnh dự báo và một ngưỡng không âm. Sau đó áp dụng dịch chuyển histogram trên phần một và phương pháp Qu trên phần hai. Cấu trúc chung của chương như sau:

#### 2.1. Tích hợp thông tin phụ trong dịch chuyển histogram

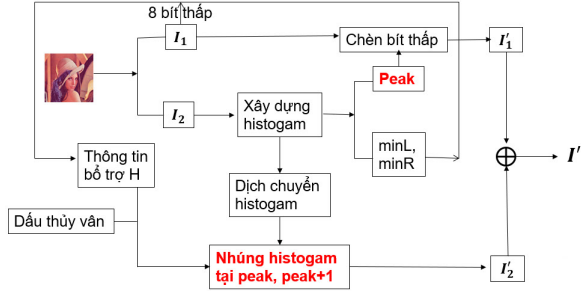
Mục này trình bày một phương pháp đề xuất (phương pháp đề xuất 1) để tích hợp các thông tin cần thiết (cho việc khôi phục tin giấu và ảnh gốc) và ảnh thủy vân.

Ý tưởng phương pháp đề xuất là chia ảnh  $I$  thành 2 miền:  $I_1$  gồm 8 điểm ảnh và  $I_2$  là phần còn lại. Sau đó xây dựng histogram  $h(x)$  trên  $I_2$ . Việc nhúng tin được thực hiện bằng phương pháp dịch chuyển histogram trên

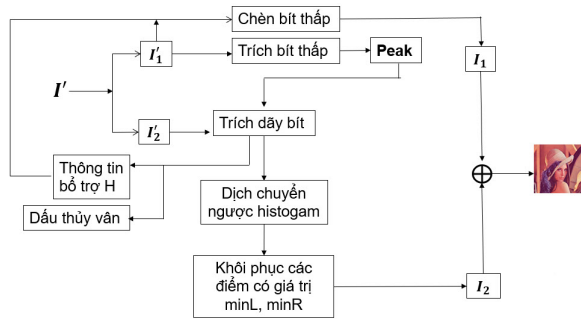


$I_2$  (chứ không phải trên  $I$ ), còn giá trị *peak* được được lưu trữ trên các bit thấp của  $I_1$ .

Sơ đồ thực hiện nhúng tin và trích tin trình bày trong Hình 2.1, 2.2.



**Hình 2.1:** Sơ đồ nhúng của đề xuất 1



**Hình 2.2:** Sơ đồ trích của đề xuất 1

**So sánh phương pháp đề xuất với các phương pháp Hwang và MF**

*Khả năng nhúng*

Ở mức 1, gấp 1.02 lần so với Hwang và gấp 2 so với MF.

Ở mức 2, gấp 1.97 lần so với Hwang và gấp 1.95 so

với MF.

Ở cả hai mức, gấp 1.34 lần so với Hwang và gấp 1.97 so với MF. *Độ phức tạp tính toán*

Khối lượng tính toán của phương pháp đề xuất ít hơn nhiều so với cả hai phương pháp Hwang và MF.

## 2.2. Giấu tin thuận nghịch sử dụng dịch chuyển histogram trên các dãy con

Mục này trình bày một đề xuất mới (đề xuất 2): chia dãy sai số dự báo thành các dãy con và áp dụng dịch chuyển histogram trên từng dãy con. Bộ dự báo sử dụng ở đây là MED, vì vậy đề xuất 2 có tên là MED-SUB.

### 2.3. Phương pháp MED-SUB

Như nhận xét ở trên, nếu chia chuỗi sai số dự báo  $E$  thành các chuỗi con có sự tương quan về độ phẳng và ứng dụng phương pháp HS cho mỗi chuỗi con một cách độc lập, khi đó có thể đạt được khả năng nhúng cao hơn khi so sánh với phương pháp MED-PEHS. Để thu được nhúng chuỗi con như vậy, dưới đây luận án sẽ sử dụng ngữ cảnh dự đoán của các điểm ảnh.

Mọi điểm ảnh  $x_i$  của ảnh gốc có ngữ cảnh dự báo gồm ba điểm ảnh  $pc_i = \{a_i, b_i, c_i\}$  và một sai số dự báo  $e_i$ . Chúng ta sẽ nhóm  $e_i$  bằng cách sử dụng mức phẳng của  $pc_i$ . Ở đây, mức phẳng này được xác định như sau:

$$FL_i = \max\{a_i, b_i, c_i\} - \min\{a_i, b_i, c_i\}.$$

$FL_i$  càng nhỏ, ngữ cảnh  $pc_i$  càng phẳng.

Để phân chia chuỗi  $E = (e_1, e_2, \dots, e_K)$  vào chuỗi con  $s$ , luận án sử dụng ngưỡng  $T_0, T_1, \dots, T_s$  như là:

$T_0 = 0, T_s = 255, T_0 < T_1 < \dots < T_{s-1} < T_s$ , và tập:

$$E^t = \{e_i \in E \mid T_t \leq FL_i < T_{t+1}\}, t = 0, 1, \dots, s-1.$$

Thay vì áp dụng phương pháp HS trên toàn miền  $E$ , luận án sử dụng phương pháp này cho các chuỗi con  $E^t$  một cách độc lập. Luận án sẽ chỉ ra rằng, phương pháp này luôn đạt được khả năng nhúng tin cao hơn. Thực tế là, nếu sử dụng các ký hiệu  $h, LPP, RPP$  như trong phần 1.2,  $h^t$  ký hiệu là histogram của chuỗi con  $E^t$  và  $LPP^t, RPP^t$  ký hiệu là hai giá trị mà  $h^t$  đạt được hai giá trị lớn nhất, khi đó các chuỗi con  $E^t$  không chồng lấp, khả năng của phương pháp MED-PEHS có thể được diễn giải như dưới đây:

$$C_{PEHS} = h(LPP) + h(RPP) = \sum_{t=0}^{s-1} (h^t(LPP) + h^t(RPP)).$$

Hơn nữa, khả năng nhúng của phương pháp MED-SUB có thể được tính bằng công thức dưới đây:

$$C_{sub} = \sum_{t=0}^{s-1} (h^t(LPP^t) + h^t(RPP^t)).$$

Theo định nghĩa, có:

$$h^t(LPP^t) + h^t(RPP^t) \geq h^t(LPP) + h^t(RPP),$$

$$t = 0, 1, \dots, s-1.$$

Như vậy, chúng ta thu được  $C_{sub} \geq C_{PEHS}$ . Lưu ý rằng ở phương pháp MED-SUB, một số thông tin phụ như  $LPP^t, RPP^t$  cần được lưu trữ. Do đó, số lượng của chuỗi con phải không quá lớn. Trong thực nghiệm,  $s = 3$  và hai ngưỡng  $t_1, t_2$  được xác định riêng lẻ cho mỗi ảnh thử nghiệm bằng cách tìm kiếm trong miền  $\{0 < t_1 < t_2 \leq 50\}$  để thu được khả năng nhúng cao nhất có thể.

## 2.4. Cải tiến phương pháp Qu (IQ)

Trong phần này, sự kết hợp phương pháp Qu và phương pháp HS được gọi là đề xuất 3 (còn gọi là IQ). Trước tiên, sử dụng một số nguyên  $t \geq 0$  để phân chia chuỗi  $E$  thành hai chuỗi con độc lập:

$$E = \begin{cases} e_i \text{ được tính theo dự báo MED,} & \text{nếu } FL_i \leq t \\ e_i \text{ được tính theo dự báo Qu,} & \text{nếu } FL_i > t \end{cases}$$

$$E_t^- = \{e_i \in E \mid FL_i \leq t\},$$

$$E_t^+ = \{e_i \in E \mid FL_i > t\},$$

với  $FL_i = \max(C_i) - \min(C_i)$  Khi đó:

$$Q(E) = Q(E_t^-) + Q(E_t^+),$$

với  $Q(E)$ ,  $Q(E_t^-)$ ,  $Q(E_t^+)$  tương ứng là khả năng nhúng của phương pháp Qu trên  $E$ ,  $E_t^-$ ,  $E_t^+$ . Phương pháp kết hợp HS và Qu được đề xuất như sau: Áp dụng phương pháp HS vào  $E_t^-$  và phương pháp Qu vào  $E_t^+$ . Khi đó, khả năng của phương pháp kết hợp, ký hiệu là  $C(t)$ , sẽ là:

$$C(t) = S(E_t^-) + Q(E_t^+),$$

với  $S(E_t^-)$  là khả năng nhúng của phương pháp HS trên  $E_t^-$ . Trong trường hợp  $t=0$ , rõ ràng  $S(E_0^-) > Q(E_0^-)$ . Nếu  $h^0$  là histogram của chuỗi con  $E_0^-$ , có

$$Q(E_0^-) = h^0(0).$$

Nói cách khác:

$$S(E_0^-) = h^0(LPP^0) + h^0(RPP^0),$$

với  $LPP^0$  và  $RPP^0$  là các giá trị mà  $h^0$  có giá trị lớn nhất. Do đó  $S(E_0^-)$  gấp khoảng hai lần  $Q(E_0^-)$ . Từ điều này, suy ra  $C(0) > Q(E)$ . Để tăng khả năng nhúng,

chúng ta cần tìm giá trị  $t$  sao cho  $C(t)$  đạt giá trị cao nhất. Do đó, phương pháp kết hợp được thực hiện như sau: Trước tiên, xác định giá trị tối ưu  $top$ :

$$top = arg \max\{C(t)|0 \leq t \leq 255\}.$$

(Giá trị của  $top$  khác nhau đối với mỗi ảnh thử nghiệm). Sau đó thực hiện phương pháp HS trên  $E_{top}^-$  và phương pháp Qu trên  $E_{top}^+$ . Kết quả thử nghiệm cho thấy phương pháp IQ không chỉ tăng khả năng nhúng mà chất lượng ảnh cũng được tăng lên so với phương pháp Qu.

Từ các kết quả thử nghiệm ở trên, có một số nhận xét như sau:

1. Cả phương pháp IQ và MED-SUB có khả năng nhúng cao nhất. Tiếp theo lần lượt là các phương pháp: MED-PEHS, Qu, và các phương pháp khác.
2. Phương pháp IQ có chất lượng ảnh cao nhất. Tiếp theo lần lượt là các phương pháp: Qu, MED-SUB, MED-PEHS, và các phương pháp khác.
3. Phương pháp MED-SUB có khả năng nhúng cao hơn và chất lượng ảnh tốt hơn phương pháp MED-PEHS.

### CHƯƠNG 3.

## THU NHỎ BẢN ĐỒ ĐỊNH VỊ TRONG PHƯƠNG PHÁP MỞ RỘNG SAI SỐ DỰ BÁO

Chương này trình bày một đề xuất mới (Đề xuất 4) dựa trên ý tưởng sắp xếp dãy sai số dự báo theo phương sai và độ lệch tâm của ngữ cảnh dự báo để thu nhỏ bản đồ định vị. Đề xuất 4 được thực hiện theo hai phương án. Trong phương án 1, đầu tiên sắp xếp theo chiều tăng của phương sai, sau đó các sai số dự báo có phương sai bằng nhau tiếp tục được sắp xếp theo chiều tăng độ lệch tâm. Phương án 2 sử dụng một đại lượng là tổ hợp phương sai và độ lệch tâm, sau đó sắp xếp các sai số dự báo theo chiều tăng dần của đại lượng này. Chương này được thiết kế như sau:

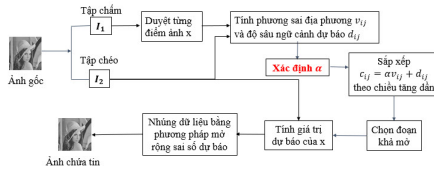
### 3.1. Giấu tin thuận nghịch dựa trên sắp xếp sai số dự báo theo phương sai và độ lệch tâm - phương án 1

Từ nhận xét về sự tương đồng giữa phương sai địa phương nhỏ và khả năng khả mở của điểm ảnh. Lược bỏ đề xuất quan tâm đến độ nhỏ của phương sai địa phương và độ lệch tâm, tức là vùng ngữ cảnh càng gần tâm miền điểm ảnh (127) thì khả năng điểm ảnh đó khả mở càng cao. Thuật toán nhúng thực hiện nhúng tin trên vùng phương sai địa phương của điểm ảnh có giá trị nhỏ. Sau khi sắp xếp để chọn ra những điểm ảnh có phương sai địa phương nhỏ với ưu tiên độ lệch tâm nhỏ từ đó xác định được vùng khả mở đầu tiên. Thực hiện

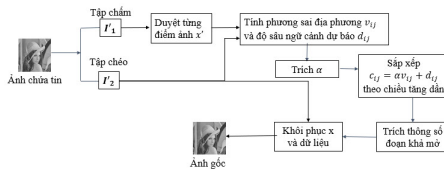
nhúng tin trên vùng khả mở này. Như vậy, bản đồ định vị được thu nhỏ chỉ còn xác định giá trị để xác định vùng khả mở.

### 3.2. Giấu tin thuận nghịch dựa trên sắp xếp sai số dự báo theo phương sai và độ lệch tâm - Phương án 2

Từ phương pháp đề xuất trong phần 3.1 về mối tương quan giữa độ lệch tâm và tính khả mở của điểm ảnh. Phần này, luận án đề xuất phương pháp thực hiện việc nhúng tin trên các điểm ảnh có phương sai địa phương nhỏ và ngữ cảnh dự báo nằm sâu bên trong miền điểm ảnh (đoạn  $[0,255]$ ) dựa trên một phương trình tuyến tính. Thuật toán nhúng tin và trích tin được trình bày trong Hình 3.1 và Hình 3.2.



**Hình 3.1:** Thuật toán nhúng tin trên một khối điểm ảnh.



**Hình 3.2:** Thuật toán nhúng tin trên một khối điểm ảnh.

## CHƯƠNG 4.

### GIẤU TIN TRÊN CÁC ĐIỂM ẢNH LỚN NHẤT VÀ NHỎ NHẤT CỦA MỖI KHỐI ẢNH BẰNG PVO

Chương này trình bày một đề xuất mới (đề xuất 5) về giấu tin thuận nghịch dựa trên PVO. Gần đây (năm 2018) Li và cộng sự đã xây dựng phương pháp GePVO-K để nhúng dữ liệu trên tất cả các điểm ảnh có giá trị lớn nhất và nhỏ nhất của mỗi khối ảnh dựa trên kỹ thuật PVO. Phương pháp đề xuất của luận án dựa trên ý tưởng của GePVO-K nhưng đưa vào nhiều cải tiến để vừa nâng cao khả năng nhúng vừa tăng chất lượng ảnh chứa tin so với GePVO-K.

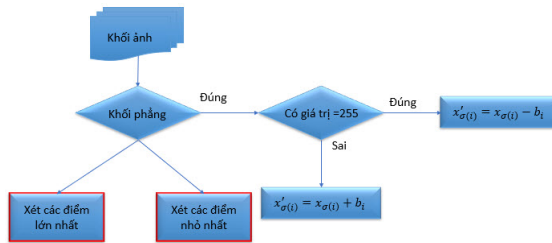
#### 4.1. Giấu tin trên các điểm ảnh lớn nhất và nhỏ nhất của mỗi khối ảnh

Trong phương pháp này, trước tiên xét mức độ phẳng của mỗi khối, sau đó sắp xếp khối điểm ảnh và thực hiện nhúng ở trên các các điểm ảnh lớn nhất và nhỏ nhất của khối.

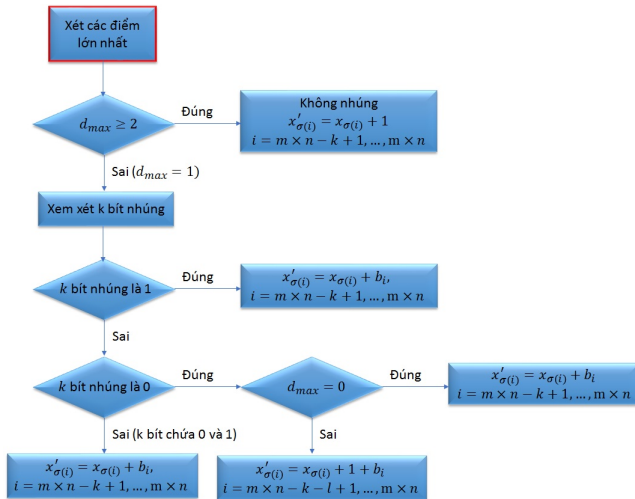
Sơ đồ nhúng tin được biểu thị trong Hình 4.1 và Hình 4.2.

Có một số lý do mà phương pháp đề xuất có khả năng nhúng cao hơn phương pháp GePVO-K. Lý do đầu tiên đó là phương pháp đề xuất có kích thước bản đồ ít hơn nhiều so với phương pháp GePVO-K. Để phân biệt ba loại khối là khối gãy tràn, khối phẳng và khối không phẳng, phương pháp GePVO-K sử dụng 2 bit để đánh dấu mỗi khối, Trong phương pháp đề xuất, có hai tình





**Hình 4.1:** Thuật toán nhúng tin trên một khối điểm ảnh.



**Hình 4.2:** Thuật toán nhúng tin ở trên các giá trị lớn nhất của khối.

huống cần phân biệt đó khối gây tràn hoặc không. Một số cờ được sử dụng để phân biệt khối phẳng hay khối có hai giá trị khác biệt, song số lượng nhỏ.

Lý do thứ hai là các khối phẳng chứa 0/255 bị bỏ qua trong phương pháp GePVO-K, nhưng trong phương pháp đề xuất chúng được sử dụng để nhúng tin.

Một lý do khác đó là số lượng bit dữ liệu được nhúng trong phương pháp đề xuất cao hơn. Điều này có được nhờ vào sự ít biến đổi ở phương pháp đề xuất. Đối với các khối có 3 giá trị khác biệt, trong phương pháp nhúng của GePVO-K cần tăng cả giá trị lớn nhất và lớn nhì, như vậy khoảng cách giữa giá trị nhỏ nhất và nhỏ thứ hai bị thay đổi, không thể nhúng thêm dữ liệu ở trường hợp nhỏ nhất. Các trường hợp khác, khả năng nhúng của hai phương pháp là tương đương.

Về chất lượng ảnh, trong phương pháp GePVO-K, trước khi nhúng, các điểm lớn nhất và lớn nhì (ở bên lớn nhất) phải tăng 1, như vậy mỗi điểm ảnh để nhúng tin có thể thay đổi tối đa 2 đơn vị. Trong phương pháp đề xuất, mỗi điểm ảnh thay đổi tối đa là 1 đơn vị. Điều này giúp cho tổng số thay đổi của phương pháp đề xuất ít hơn nhiều so với phương pháp GePVO-K. Rõ ràng, chất lượng ảnh của phương pháp đề xuất tốt hơn so với phương pháp GePVO-K.

## KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

### Các đóng góp chính

Luận án đã có những đóng góp sau:

Thứ nhất, theo hướng dịch chuyển histogram, luận án đã đưa ra được ba đề xuất mới:

Đề xuất thứ nhất là một giải pháp tích hợp mọi thông tin dùng trong quá trình khôi phục vào ảnh chứa tin. Như vậy người nhận chỉ cần dùng ảnh chứa tin để tính dữ liệu và khôi phục ảnh gốc. Ngoài ra, phương pháp này cũng đưa ra cách lựa chọn cặp histogram tối ưu để tăng khả năng nhúng tin.

Đề xuất thứ hai là ý tưởng chia dãy sai số dự báo thành các dãy con tương đối phẳng bằng cách sử dụng độ phẳng của ngữ cảnh dự báo. Sau đó áp dụng dịch chuyển histogram trên dãy con này.

Đề xuất thứ 3 là một sự kết hợp dịch chuyển histogram và phương pháp Qu. Dãy sai số dự báo được chia làm hai phần dựa vào độ phẳng của ngữ cảnh dự báo và một ngưỡng không âm. Phần đầu sử dụng dịch chuyển histogram và phần còn lại áp dụng phương pháp Qu.

Thứ hai, theo hướng mở rộng hiệu, luận án đưa ra một đề xuất mới để thu nhỏ bản đồ định vị bằng cách sắp xếp sai số dự báo theo thứ tự tăng của phương sai và độ lệch tâm ngữ cảnh dự báo.

Cuối cùng, theo hướng PVO, luận án đưa ra một đề xuất mới là nhúng tin trên tất cả các điểm ảnh có giá trị lớn nhất và nhỏ nhất của một khối ảnh sau khi sắp xếp theo PVO.

Bằng phân tích lý thuyết và kết quả thực nghiệm chứng tỏ các phương pháp đề xuất mới trong luận án có nhiều điểm ưu việt hơn khi so sánh với các phương pháp liên quan hiện có.

## **Hạn chế của luận án**

Do giấu tin và thủy vân là một lĩnh vực rộng trên nhiều phương tiện mang tin như ảnh số, âm thanh số, video số, dữ liệu số. Tuy nhiên, luận án chỉ dừng lại ở mức giấu tin trên ảnh số đa mức xám, là một lĩnh vực được quan tâm nhiều nhất tại thời điểm này.

## **Một số hướng phát triển**

Tiếp theo hướng nghiên cứu giấu tin trên ảnh số, tác giả luận án tiếp tục khai thác sâu hơn. Ảnh mang tin không chỉ dừng lại ở ảnh đa mức xám, mà sẽ nghiên cứu thêm về ảnh nén, ảnh jpeg, ảnh vệ tinh, ảnh y tế,... là các lĩnh vực hiện rất được sự quan tâm vì tính ứng dụng cao của chúng trong thực tế.

## CÁC CÔNG TRÌNH KHOA HỌC ĐÃ CÔNG BỐ

**Danh mục các công trình khoa học của tác giả  
liên quan đến luận án**

- NKS1 . **Sao Nguyen, Kim**, Quang Hoa Le, and Van At Pham (2017). “ A New Reversible Watermarking Method Based on Histogram Shifting” Applied Mathematical Sciences 11.10 pp.445-460.
- NKS2 . **Nguyễn Kim Sao**, Đỗ Văn Tuấn, Phạm Văn Át (2018), “Giấu tin thuận nghịch sử dụng các thuộc tính của ngữ cảnh dự báo để loại bỏ bản đồ định vị”, Tạp chí Công nghệ thông tin và truyền thông, p10-18.
- NKS3 . **Nguyễn Kim Sao**, Cao Thị Luyên (12/2017), “ Thủy vân thuận nghịch dựa trên dự báo, sắp xếp phương sai và độ lệch tâm”, Khoa học và công nghệ quân sự, Số đặc san CNTT.
- NKS4 . **Nguyễn Kim Sao**, Nguyen Ngoc Hoa, Pham Van At (2019), An effective reversible data hiding method based on pixel-value-ordering - Journal of Computer Science and Cybernetics (đã được chấp nhận)
- NKS5 . **Nguyen Kim Sao**, Cao Thi Luyen, Le Kinh Tai, and Pham Van At. Reversible data hiding based on prediction error histogram shifting and pixel-based PVO - ACIIDS 2020 (đã được chấp nhận)

Danh mục này gồm 05 công trình.