

Phát hiện ảnh giấu tin sử dụng kỹ thuật giấu thuận nghịch dựa trên dịch chuyển Histogram

Hồ Thị Hương Thom^{1,*}, Hồ Văn Canh², Trịnh Nhật Tiến³

¹Khoa công nghệ thông tin, Trường Đại học dân lập Hải Phòng, Hải Phòng, Việt Nam

²Cục kỹ thuật nghiệp vụ I - Bộ Công An, Hà Nội, Việt Nam

³Trường Đại học Công nghệ, Đại học Quốc gia Hà Nội, Hà Nội, Việt Nam

Nhận ngày 10 tháng 9 năm 2010

Tóm tắt. Trong thời gian gần đây giấu thuận nghịch được quan tâm một cách đặc biệt. Vào năm 2007, Hwang và các đồng nghiệp đề xuất kỹ thuật giấu thuận nghịch (HKC) [9] cải tiến phương pháp giấu của Ni (NSAS) [7] dựa trên dịch chuyển histogram của ảnh. Tuy nhiên kỹ thuật giấu này tạo ra một sự phân bố không bình thường trên histogram của ảnh sau khi thông điệp được giấu. Kuo và các đồng nghiệp của ông đã nêu ra vấn đề không an toàn của kỹ thuật này và đề xuất kỹ thuật phát hiện tương ứng. Nhưng kỹ thuật họ đề xuất chỉ có thể phát hiện khi ảnh được giấu với lượng thông điệp giấu lớn 100% khả năng của kỹ thuật HKC, trong một số trường hợp khác nó không thể phát hiện. Vì vậy nhóm tác giả đưa ra một số cải tiến phù hợp để có thể phát hiện cho các trường hợp giấu với lượng thông điệp giấu khác nhau sử dụng kỹ thuật giấu HKC.

Từ khoá: Steganography, steganalysis, stego-image, cover-image, LSB.

1. Giới thiệu

Trong thời gian gần đây giấu tin mật trong đa phương tiện ngày càng trở nên phổ biến trong môi trường truyền thông công cộng. Khác với mã hoá thông tin làm cho bản thông điệp được biết rõ là đã bị mã hoá, ngược lại giấu tin trong đa phương tiện làm cho các đối tượng mang tin mật khó có thể bị phát hiện bằng kỹ thuật thông thường, vì nó không làm thay đổi nhiều nội dung ban đầu của đối tượng mang thông điệp. Phương pháp giấu tin đơn giản nhất là thông điệp dưới dạng nhị phân sẽ được nhúng “thay thế” vào các bit LSB (Least

Signification Bit – Bit có trọng số thấp) của ảnh như các kỹ thuật đã công bố [1-5]. Tuy nhiên với các kỹ thuật này, sau khi tách thông điệp, khó khôi phục lại được ảnh gốc ban đầu.

Một vài lĩnh vực như y học, quân đội hoặc nghiên cứu thực nghiệm vật lý phân tử hạt nhân, ... nó đòi hỏi không những tách đúng thông điệp mà còn khôi phục xấp xỉ đúng ảnh gốc ban đầu. Vào năm 2001, phương pháp giấu thuận nghịch đầu tiên được đề xuất bởi Honsinger cùng các đồng nghiệp [6], từ đó đến nay nhiều kỹ thuật giấu thuận nghịch được công bố với hai hình thức giấu chính là trong miền dữ liệu và trong miền dữ liệu biến đổi.

Gần đây, kỹ thuật giấu thuận nghịch (NSAS) dựa trên dịch chuyển histogram của

* Tác giả liên hệ. ĐT: 84-31-3593816.
E-mail: thomhth@hpu.edu.vn

ảnh được do Ni và các đồng nghiệp đề xuất [7], họ chỉ ra rằng kỹ thuật giấu này có độ phức tạp tính toán thấp, không làm thay đổi nhiều nội dung ảnh. Sau đó để nâng cao lượng thông điệp giấu trong ảnh, Hwang và các đồng nghiệp đề xuất kỹ thuật HKC [8] dựa trên cải tiến kỹ thuật của Ni để có thể giấu thông điệp với lượng giấu lớn hơn kỹ thuật NSAS.

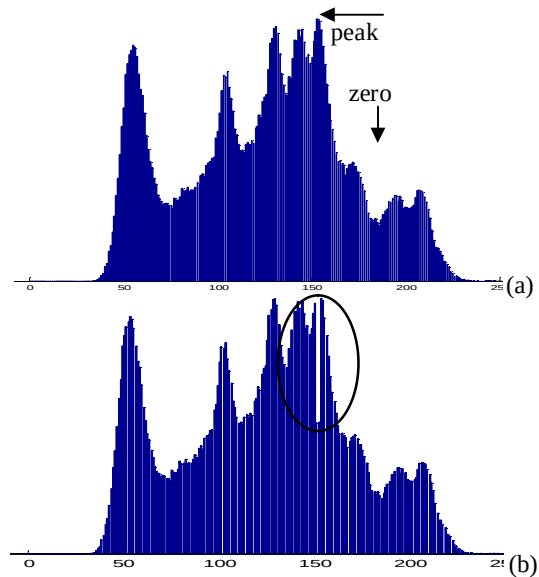
Các kỹ thuật này mặc dù không làm thay đổi nhiều trực quan của vật mang tin, nhưng nó để lại một dấu hiệu không bình thường trên lược đồ histogram của các ảnh đó. Vì vậy dựa trên quan sát một loạt histogram của các ảnh trước và sau khi giấu tin bằng các kỹ thuật trên, Kuo và các đồng nghiệp của ông đã đưa ra vấn đề không an toàn của kỹ thuật giấu HKC và đề xuất kỹ thuật phát hiện tương ứng [9].

Trong phần 2, nhóm tác giả sẽ trình bày lại thuật toán giấu tin NSAS, HKC. Phần 3 trình bày kỹ thuật phát hiện của Kuo cho kỹ thuật HKC, sau đó chúng tôi đưa ra một số trường hợp không thể phát hiện ảnh có giấu tin sử dụng kỹ thuật HKC do Kuo đưa ra và đề xuất kỹ thuật phát hiện cải tiến phù hợp cho mọi trường hợp giấu sử dụng HKC. Cuối cùng đưa ra kết quả thử nghiệm và kết luận trong phần 4 và phần 5

2. Một số lược đồ giấu tin dựa trên histogram

2.1 Kỹ thuật giấu thuận nghịch NSAS

Vào năm 2006, Ni và các đồng nghiệp đã đề xuất lược đồ giấu tin thuật nghịch NSAS trên ảnh dựa trên dịch chuyển histogram của ảnh [7]. Theo kỹ thuật của Ni, quá trình giấu tin gồm các bước sau đây:



Hình 1. (a) Histogram ảnh gốc, (b) Histogram ảnh giấu tin.

Thuật toán giấu thuật nghịch NSAS

Bước 1. Tìm một điểm zero (điểm không) và một điểm peak (điểm cực trị). Điểm zero và điểm peak là điểm có giá trị cấp xám của pixel trong lược đồ histogram của ảnh nhỏ nhất và bằng cực đại. Hình 1 là ví dụ minh họa cho kỹ thuật này (a) histogram của ảnh lena trước khi giấu tin. Để đơn giản ví dụ điểm zero ở vị trí 255 ($h(255)=0$) và điểm peak ở 154 ($h(154)=2859$).

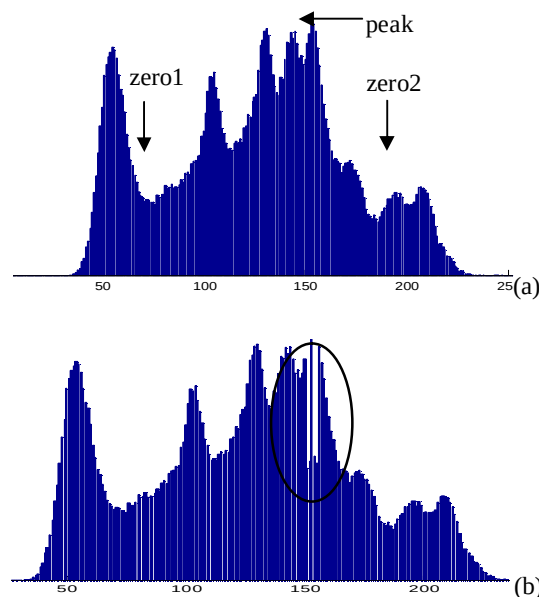
Bước 2. Quét toàn bộ ảnh theo thứ tự: trái sang phải, từ trên xuống. Các pixel có giá trị xám nằm trong khoảng [155 254] được tăng lên một giá trị. Nó sẽ làm cho tần số của 155 bằng 0.

Bước 3. Nhúng bit thông điệp “0” và “1” lần lượt vào các giá trị xám 154 và 155 theo nguyên tắc sau: Giả sử pixel đang xét là 154 kiểm tra bit cần nhúng, nếu là bit “1” thì pixel 154 sẽ tăng lên 1, ngược lại nếu là bit “0” thì pixel 154 vẫn giữ nguyên. Hình 1 (b) Histogram của ảnh sau khi giấu tin.

Cuối cùng chúng ta nhận được ảnh stego-image, sau đó chúng ta có thể chuyển đến người nhận thông qua internet. Người nhận có thể khôi phục lại thông điệp và ảnh gốc bằng kỹ thuật biến đổi ngược, người đọc có thể xem [7] để biết thêm chi tiết cách tách thông điệp.

2.2. Kỹ thuật giấu thuật nghịch HKC

Trong kỹ thuật NSAS, chúng ta thấy khả năng giấu thông điệp phụ thuộc vào độ lớn của điểm peak, như với ví dụ trên khả năng giấu lượng thông điệp không quá 2859 bit trong ảnh. Tuy nhiên làm thế nào để truyền thông tin về điểm zero và điểm peak hay thông tin bổ sung thông điệp giấu từ người gửi đến người nhận là không được đề cập trong tài liệu này. Để cải tiến vấn đề này, Hwang và các đồng nghiệp của ông đề xuất kỹ thuật giấu thuật nghịch HKC [8].



Hình 2. (a) Histogram ảnh gốc,
(b) Histogram ảnh giấu tin.

Thuật toán giấu thuật nghịch HKC

Bước 1. Tìm ra một điểm peak (giả sử đó là vị trí 154 trong ảnh ví dụ Lena) và hai điểm min (đó là vị trí 23 và 255). Điểm peak và các điểm min tương ứng với số pixel của chúng là lớn nhất và nhỏ nhất trong ảnh (xem hình 2 (a)).

Bước 2. Nhằm để khôi phục chính xác ảnh gốc, một bản đồ định vị được đề xuất dùng để lưu trữ thông tin vị trí của các pixel (như là điểm peak, điểm min bên trái điểm peak, lượng pixel ban đầu của điểm min bên trái, điểm min bên phải điểm peak, lượng pixel ban đầu của điểm min bên phải) trong lược đồ HKC.

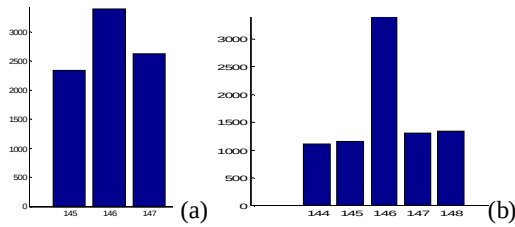
Bước 3. Khởi tạo không gian để nhúng tin. Các pixel được định vị trong histogram nằm ở bên trái giữa điểm peak và điểm min bên trái sẽ dịch sang trái một pixel. Tương tự, các pixel được định vị nằm ở bên phải giữa điểm peak và điểm min bên phải sẽ dịch sang phải một pixel.

Bước 4. Nhúng thông tin vào trong ảnh. Nếu pixel đang xét có giá trị bằng peak-2 hoặc peak +2 thì kiểm tra bit cần nhúng trong chuỗi bit thông điệp: nếu bit thông điệp là 1 thì pixel có giá trị là peak-2 sẽ tăng lên 1, pixel có giá trị là peak+2 sẽ giảm đi 1, còn nếu bit thông điệp là 0 thì vẫn duy trì như cũ. Hình 2 (b) histogram của ảnh sau khi giấu tin.

3. Phương pháp phát hiện ảnh có giấu tin

3.1. Tấn công kỹ thuật HKC của Kuo

Năm 2008, Kuo và các đồng nghiệp của ông đề xuất kỹ thuật phát hiện ảnh có giấu tin sử dụng kỹ thuật giấu HKC [9]. Nhóm tác giả quan sát histogram dựa vào đỉnh peak trước và sau khi giấu thấy hai giá trị lân cận hai bên của đỉnh peak bị tụt xuống do giấu tin như mô tả trong hình 3 (a) và (b), vì vậy họ đưa ra định lý 1 để xây dựng kỹ thuật phát hiện dưới đây.



Hình 3. Điểm Peak: (a) trước khi giấu tin, (b) sau khi giấu tin.

Định lý 1: Có 5 cặp giá trị liên tiếp (x_1, y_1) , (x_2, y_2) , (x_3, y_3) , (x_4, y_4) , (x_5, y_5) với (x_3, y_3) là cặp giá trị điểm peak. Tỷ lệ thay đổi của 5 điểm liên tục và mối quan hệ láng giềng được định nghĩa lần lượt như biểu thức (1) và (2):

$$\frac{y_3 - y_2}{y_3} \approx \frac{y_3 - y_4}{y_3} \approx \tau_1, 0.4 \leq \tau_1 \leq 0.6 \quad (1)$$

$$\left| \frac{y_1 - y_2}{y_2} \right| \approx \left| \frac{y_4 - y_5}{y_4} \right| \leq \tau_2 \quad (2)$$

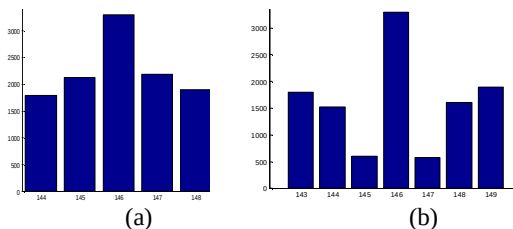
τ_2 là giá trị ngưỡng (trong [9], tác giả lấy $\tau_2 = 0.1$).

Áp dụng định lý này, Kuo đưa ra thuật toán phát hiện ảnh có giấu tin sử dụng kỹ thuật HKC theo các bước sau:

Bước 1. Tìm cặp giá trị điểm peak $(x_{\max}, y_{\max})$

Bước 2. Tính tỉ lệ thay đổi và mối quan hệ láng giềng bằng cách sử dụng định lý 1.

Bước 3. Nếu 5 cặp giá trị liên tiếp lân cận $(x_{\max}, y_{\max})$ thỏa mãn (1) và (2), thì kết luận ảnh có giấu tin trong vùng này, ngược lại ảnh không giấu tin.



Hình 4. Histogram của: (a) ảnh gốc, (b) ảnh giấu tin bằng HKC.

Với kỹ thuật phát hiện của Kuo (dựa trên định lý 1) trong một số trường hợp giấu tin của HKC chúng tôi thấy không phù hợp khi thông điệp không được giấu hết vào vị trí của cột peak. Ví dụ như hình 4 (a) điểm peak là 146, sau khi giấu tin hai cột giá trị lân cận peak là 145 và 147 bị tụt xuống, nhưng lượng bit giấu ít hơn độ lớn của 2 điểm này cho nên giá trị của 144 không bằng 145 và giá trị 147 không bằng 148 (xem hình 4 (b)), theo ví dụ ta có $y_1=1520$, $y_2=600$, $y_3=3300$, $y_4=580$, $y_5=1600$

Trong trường hợp này kiểm tra lại biểu thức (1) và (2) ta thấy $(y_3 - y_2)/y_3 = 0.8182$ và $(y_3 - y_4)/y_3 = 0.8242$

$$\text{và } \left| \frac{y_1 - y_2}{y_2} \right| = 1.5333 \quad \text{và} \quad \left| \frac{y_4 - y_5}{4} \right| = 1.7586$$

không thỏa mãn (1) và (2)

Để có thể phát hiện một cách tổng quát hơn với kỹ thuật của Kuo chúng tôi đưa ra định lý 2 chỉnh sửa của Kuo như sau:

Định lý 2: Có 5 cặp giá trị liên tiếp (x_1, y_1) , (x_2, y_2) , (x_3, y_3) , (x_4, y_4) , (x_5, y_5) trong đó (x_3, y_3) là cặp giá trị điểm peak. Tỷ lệ thay đổi của 5 điểm liên tục và mối quan hệ láng giềng được định nghĩa lần lượt như biểu thức (1') và (2'):

$$\frac{y_3 - y_2}{y_3} \approx \frac{y_3 - y_4}{y_3} \approx \tau_1, 0.4 \leq \tau_1 \leq 1 \quad (1')$$

$$\left| \frac{y_1 - y_2}{y_2} \right| \approx \left| \frac{y_4 - y_5}{4} \right| \quad (2')$$

3.2. Kỹ thuật phát hiện đề xuất

Mặt khác chúng tôi thấy có thể đưa ra biểu thức đơn giản hơn phát hiện ảnh có giấu tin sử dụng kỹ thuật giấu HKC. Dựa vào phân tích ví dụ trên: ảnh gốc ban đầu có histogram như hình 4 (a) tổng hai cột giá trị lân cận (h_{144}, h_{146}) bên trái và hai cột giá trị lân cận bên phải (h_{147}, h_{148}) của điểm Peak (h_{146}) luôn lớn hơn Peak (tức $h_{144} + h_{145} > h_{146}$, $h_{147} + h_{148} > h_{146}$), trong khi với

histogram của ảnh có giấu tin hình 4 (b) thì $h_{144}+h_{145} < h_{146}$, $h_{147}+h_{148} < h_{146}$. Vì vậy chúng tôi đưa ra định lý 3 dưới đây.

Định lý 3: Có 5 cặp giá trị liên tiếp (x_1, y_1) , (x_2, y_2) , (x_3, y_3) , (x_4, y_4) , (x_5, y_5) với điểm Peak (điểm max) là (x_3, y_3) . Khi đó mối quan hệ lằng giềng của năm điểm này được định nghĩa như sau:

$$y_1 + y_2 < y_3 \quad (3)$$

$$y_4 + y_5 < y_3 \quad (4)$$

Áp dụng định lý 3 chúng ta có thể xây dựng các thuật toán phát hiện ảnh có giấu tin bằng kỹ thuật HKC.

Thuật toán phát hiện ảnh có giấu tin bằng kỹ thuật giấu HKC:

Bước 1: Thống kê tần số pixel của ảnh. Tìm điểm Peak có số pixel lớn nhất $(x_{\max}, y_{\max})$.

Bước 2: Tìm 2 cặp điểm liên tiếp bên trái $(x_{\max-2}, y_{\max-2})$, $(x_{\max-1}, y_{\max-1})$ và liên tiếp phải $(x_{\max+1}, y_{\max+1})$, $(x_{\max+2}, y_{\max+2})$.

Bước 3. Nếu 5 điểm $(x_{\max-2}, y_{\max-2})$, $(x_{\max-1}, y_{\max-1})$, $(x_{\max}, y_{\max})$, $(x_{\max+1}, y_{\max+1})$, $(x_{\max+2}, y_{\max+2})$ thỏa mãn biểu thức (3) và (4) thì chúng ta có thể phát hiện thông điệp được giấu trong vùng này. Ngược lại, có thể kết luận ảnh này không giấu tin.

4. Kết quả thử nghiệm và đánh giá

a) Độ đo đánh giá

Trong những thử nghiệm này, chúng tôi sử dụng các độ đo đánh giá là: *precision*, *recall* và *f-measure* thường được áp dụng trong phân loại dữ liệu. *Precision* là độ đo tính chính xác và đúng đắn của việc phân loại. *Recall* là độ đo tính toàn vẹn của việc phân lớp.

Cụ thể cho bài toán phân loại ảnh có giấu tin và ảnh chưa giấu tin, giả sử ta có một tập ảnh đầu vào E (gồm cả ảnh giấu tin và ảnh chưa

giấu tin) cần phân thành 2 tập con E_1 (ảnh có giấu tin) và E_2 (ảnh không giấu tin). Sau khi thực hiện phân lớp chúng ta được bảng sau:

		Kết quả phân lớp đúng	
		E_1	E_2
Kết quả phân lớp đạt được	E_1	tp (true positive)	fp (false positive)
	E_2	fn (false negative)	tn (true negative)

Khi đó *precision* và *recall* được tính toán theo công thức sau:

$$\text{Precision} = \frac{tp}{tp + fp} \quad (5)$$

$$\text{Recall} = \frac{tp}{tp + fn} \quad (6)$$

Mặc dù *precision* và *recall* là những độ đo được dùng rộng rãi và phổ biến nhất, nhưng chúng lại gây khó khăn khi phải đánh giá các bài toán phân loại vì hai độ đo trên lại không tăng/giảm tương ứng với nhau. Bài toán đánh giá có *recall* cao có thể có *precision* thấp và ngược lại. Hơn nữa, việc so sánh mà chỉ dựa trên một mình *precision* và *recall* không phải là một ý hay. Với mục tiêu này, độ đo *F-measure* được sử dụng để đánh giá tổng quát các bài toán phân loại. *F-measure* là trung bình điều hoà có trọng số của *precision* và *recall* và có công thức:

$$F_{\beta} = (1 + \beta^2) \cdot \frac{\text{precision} \cdot \text{recall}}{\beta^2 \cdot \text{precision} + \text{recall}}$$

trong đó β là một tham số có giá trị nằm giữa 0 và 1. Nếu $\beta = 1$, *F-measure* bằng với *precision* và nếu $\beta=0$, *F-measure* bằng với *recall*. Giữa đoạn đó, giá trị β càng cao, độ quan trọng của *precision* càng cao so với *recall*. Chúng tôi sử dụng giá trị thường được dùng là $\beta = 0.5$, nghĩa là

$$F = 2 \cdot \frac{\text{precision} \cdot \text{recall}}{\text{precision} + \text{recall}} \quad (7)$$

b) Kết quả thử nghiệm

Để thử nghiệm chương trình, chúng tôi sử dụng Matlab R2007b với tập dữ liệu gồm 100 ảnh xám trong đó 50 ảnh được lấy về từ [10] và 50 ảnh được tạo ra từ máy ảnh kỹ thuật số. Chúng tôi đem nhúng cùng một thông điệp

bằng kỹ thuật HKC được tập ảnh mới ký hiệu là *tập dữ liệu ảnh 1* gồm 200 ảnh với 100 ảnh gốc ban đầu và 100 ảnh có giấu tin. Sau đó sử dụng kỹ thuật phát hiện HKC của Kuo, kỹ thuật Kuo có chỉnh sửa và kỹ thuật do chúng tôi đề xuất được kết quả đánh giá trong bảng 1.

Bảng 1. Kết quả thử nghiệm trên tập dữ liệu ảnh 1

Kỹ thuật \ Độ đo	Precision	Recall	F-measure
kỹ thuật của Kuo tấn công HKC	0/100 = 0	0/2 = 0	Không xác định
Kỹ thuật của Kuo có chỉnh sửa tấn công HKC	95/100 = 0.95	95/102 = 0.93	0.940
Kỹ thuật đề xuất tấn công HKC	97/100 = 0.97	97/102 = 0.95	0.96

Sau đó chúng tôi tiến hành một thử nghiệm sử dụng 100 ảnh gốc ban đầu tiến hành giấu hết thông điệp (các bit được sinh ngẫu nhiên) vào các điểm lân cận điểm cực trị của ảnh gốc bằng kỹ thuật giấu HKC ta được tập dữ liệu mới là

tập dữ liệu ảnh 2 rồi tiến hành thử nghiệm phát hiện bằng 3 kỹ thuật: Kỹ thuật của Kuo, Kỹ thuật của Kuo chỉnh sửa, kỹ thuật đề xuất ta được kết quả đưa ra trong bảng 2.

Bảng 2. Kết quả thử nghiệm trên tập dữ liệu ảnh 2

Kỹ thuật \ Độ đo	Precision	Recall	F-measure
kỹ thuật của Kuo cho HKC	68/100 = 0.68	68/82 = 0.83	0.75
kỹ thuật của Kuo chỉnh sửa cho HKC	97/100 = 0.97	97/104 = 0.93	0.95
kỹ thuật đề xuất cho HKC	97/100 = 0.97	97/102 = 0.95	0.96

5. Kết luận

Từ kết quả thực nghiệm của bảng 1 và bảng 2 chúng ta có thể dễ dàng thấy rằng kết quả phát hiện do Kuo đưa ra có hiệu quả phát hiện thấp hơn sau khi được chỉnh sửa lại một số tham số. Và kỹ thuật do chúng tôi đề xuất có thể phát hiện tin cậy hơn của họ và cho mọi trường hợp giấu tin sử dụng HKC với các lượng giấu khác nhau.

Công việc tiếp theo, chúng tôi sẽ nghiên cứu một số kỹ thuật phát hiện ảnh có giấu tin sử

dụng các kỹ thuật giấu thuận nghịch khác công bố trong thời gian gần đây.

Tài liệu tham khảo

- [1] C. C. Chang, J.Y. Hsiao, and C. S. Chan, "Finding optimal LSB Substitution in image hiding by dynamic programming strategy", *Pattern Recognition*, vol. 36, no. 7 (2003) 1583.
- [2] Z. M. Lu, J. S. Pan, S. H. Sun, "VQ-based digital image watermarking method," *Electron. Lett.*, Vol. 36, no. 14(2000) 1201.

- [3] H. C. Wu, N. I. Wu, C. S. Tsai, M. S. Hwang, "Image Steganographic scheme based on pixel-value differencing and LSB replacement methods," *IEE Proc.-Vis. Image Signal Process.*, Vol. 152, Issue 5 (2005) 611.
- [4] S. H. Liu, T. H. Chen, H. X. Yao and W. Gao, "A variable depth LSB data hiding technique in images," *Machine Learning and Cybernetics*, 2004, pp. 3990-3994.
- [5] C. I. Podilchuk, E. J. Delp, "Digital watermarking: Algorithms and applications", *IEEE Signal Process. Mag.*, vol. 18, no. 4 (2001) pp. 33-34.
- [6] C. W. Honsinger, P. Jones, M. Rabbani, J. C. Stoffel, "Lossless recovery of an original image containing embedded data", US Patent application, Docket no: 77102/E-D, 2001.
- [7] Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, and Wei Su, "Reversible Data Hiding", *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 16, No.3 (2006) 354.
- [8] J.H. Hwang, J. W. Kim, J. U. Choi, "A Reversible Watermarking Based on Histogram Shifting", *IWDW 2006, LNCS 4283* (2006) pp. 384-361.
- [9] Wen-Chung Kuo, Yan-Hung Lin, "On the Security of Reversible Data Hiding Based-on Histogram Shift", *ICICIC 2008, ISSN/ISBN 9780-769531618* (2008) pp. 174-177.
- [10] USC-SIPI Image Database, "<http://sipi.usc.edu/services/database/Database.html>".

Steganalysis of Reversible Data Hiding Based on Histogram Shift

Ho Thi Huong Thom¹, Ho Van Canh², Trinh Nhat Tien³

¹*Faculty of Information Technology, Haiphong Private University, Haiphong, Vietnam*

²*Dept. of Professional Technique I, Ministry of Public Security, Hanoi, Vietnam*

³*College of Technology, Vietnam National University, Hanoi, Vietnam*

Recently, reversible data hiding scheme have been interesting specially. In 2007, Hwang et al proposed a reversible data hiding (it calls HKC) [9] which improved Ni et al's technique (NSAS) [7] based on the histogram shift. However, the technique creates an informal distribution in the histogram after hiding message into a cover image. In 2008, Kuo et al gave some insecurities of HKC technique and introduced the steganalysis for the technique. Nevertheless, their method only detect stego images with payload of 100% capacity of HKC technique, otherwise it can't detect. Therefore, we give some improvement to detect stego images using HKC steganography with various payloads.