

## **LỜI CAM ĐOAN**

Tôi xin cam đoan đây là công trình nghiên cứu của riêng tôi. Các kết quả được viết chung với các tác giả khác đều được sự đồng ý của các đồng tác giả trước khi đưa vào luận án. Các kết quả nêu trong luận án là trung thực và chưa từng được ai công bố trong bất kỳ các công trình khoa học nào khác.

*Hà Nội, tháng 4 năm 2012*

**Tác giả**

***NCS. Hồ Thị Hương Thơm***

## LỜI CẢM ƠN

Thực hiện luận án tiến sĩ là một thử thách lớn, đòi hỏi sự kiên trì và tập trung cao độ. Tôi thực sự hạnh phúc với kết quả đạt được trong đề tài nghiên cứu của mình. Những kết quả đạt được không chỉ là nỗ lực của cá nhân, mà còn có sự hỗ trợ và giúp đỡ của tập thể giáo viên hướng dẫn, cơ sở đào tạo, đơn vị công tác, đồng nghiệp và gia đình. Tôi muốn bày tỏ tình cảm của mình đến với họ.

Tôi xin bày tỏ lòng biết ơn sâu sắc tới thầy giáo TS. Hồ Văn Canh, người đã có những định hướng giúp tôi thành công trong việc nghiên cứu của mình. Thầy cũng đã động viên và chỉ bảo giúp tôi vượt qua những khó khăn để tôi hoàn thành được luận án này. Tôi cũng xin chân thành cảm ơn tới thầy PGS. TS. Trịnh Nhật Tiến, Thầy đã cho tôi những kiến thức quý báu về nghiên cứu khoa học. Nhờ sự chỉ bảo của Thầy tôi mới hoàn thành tốt luận án.

Tôi cũng muốn được bày tỏ lòng biết ơn đối với tập thể các thầy cô khoa Công nghệ thông tin, trường Đại học Công nghệ đã giúp đỡ và tạo điều kiện cho tôi rất nhiều trong quá trình học tập và nghiên cứu ở khoa; đặc biệt PGS. TS Hà Quang Thụy, TS. Nguyễn Ngọc Hóa và PGS. TS. Đỗ Năng Toàn đã có những lời khuyên quý giá trong quá trình làm NSC và viết luận án này, cảm ơn Phòng quản lý Sau đại học về sự hỗ trợ các thủ tục hoàn thành luận án.

Tôi cũng đặc biệt cảm ơn tập thể cán bộ giảng viên khoa Công nghệ Thông tin, ban Giám hiệu – Trường Đại Học Dân Lập Hải Phòng đã tận tình giúp đỡ, tạo điều kiện, hỗ trợ tôi triển khai các ý tưởng nghiên cứu trong suốt thời gian làm luận án.

Nhân dịp này, tôi cũng xin gửi lời cảm ơn sâu sắc tới gia đình, chồng con người thân và bạn bè đã cho tôi điểm tựa vững chắc để tôi có thể hoàn thành khóa học NCS.

## TÓM TẮT

Giấu thông tin (Steganography) là kỹ thuật giấu thông tin quan trọng vào đối tượng dữ liệu số khác. Phát hiện dữ liệu số giấu thông tin (Steganalysis) là kỹ thuật nhằm phân biệt dữ liệu số nào đó có giấu tin hay không. Lĩnh vực này đã và đang thu hút sự quan tâm của nhiều nghiên cứu trên thế giới, đặc biệt trong lĩnh vực an ninh, quốc phòng, thương mại, ... Phát hiện dữ liệu số giấu tin cho phép chúng ta có thể (i) phân loại dữ liệu số thu nhận được đâu là dữ liệu gốc và dữ liệu giấu tin (ii) đánh giá được mức độ an toàn của kỹ thuật giấu đã biết nào đó.

Trong luận án này, dựa trên những điểm còn hạn chế của kỹ thuật phát hiện ảnh giấu tin khác hay kỹ thuật giấu tin trong ảnh nào đó đã biết, luận án tập trung vào việc cải tiến và đề xuất một số phương pháp phát hiện với hai lớp kỹ thuật:

- Lớp kỹ thuật phát hiện mù (blind steganalysis) ứng dụng trong việc phát hiện tin giấu trên các bit ít quan trọng nhất của điểm ảnh (LSB - Least Significant Bit). Ở đây luận án đã đưa ra được một số cải tiến và đề xuất với những kỹ thuật cụ thể như dựa trên phân tích độ lệch chuẩn, thống kê  $\chi^2$  một bậc tự do, phân tích tỉ lệ xám, ước lượng thông tin giấu bằng lý thuyết trùng khớp.
- Lớp kỹ thuật phát hiện có ràng buộc (constraint steganalysis) ứng dụng trong những trường hợp chúng ta biết trước kỹ thuật giấu tin trong ảnh. Dựa trên bốn kỹ thuật giấu tin điển hình hiện nay: HKC, DIH, IWH và RVH, chúng tôi đã đề xuất tương ứng bốn giải pháp để phát hiện tin giấu trong ảnh.

Đối với cả hai lớp kỹ thuật trên, các kết quả thực nghiệm thu được đã khẳng định được tính đúng đắn của những kỹ thuật cải tiến cũng như các giải pháp phát hiện ảnh giấu tin của luận án. Kết quả bước đầu của luận án sẽ cho phép mở rộng và phát triển tiếp những công cụ, hệ thống hỗ trợ phát hiện giấu tin trên những loại dữ liệu số khác, phục vụ bài toán an toàn thông tin trong lĩnh vực an ninh, quốc phòng...

# MỤC LỤC

|  |           |
|--|-----------|
| <b>LỜI CAM ĐOAN</b> .....  | <b>1</b>  |
| <b>LỜI CẢM ƠN</b> .....  | <b>2</b>  |
| <b>MỤC LỤC</b> .....   | <b>4</b>  |
| <b>DANH MỤC CÁC KÝ HIỆU VÀ TỪ VIẾT TẮT</b> .....   | <b>7</b>  |
| <b>DANH MỤC CÁC BẢNG</b> .....   | <b>8</b>  |
| <b>DANH MỤC CÁC HÌNH VẼ</b> .....  | <b>10</b> |
| <b>PHẦN MỞ ĐẦU</b> .....   | <b>12</b> |
| <b>CHƯƠNG 1. GIẤU TIN TRONG ẢNH, PHÁT HIỆN ẢNH CÓ GIẤU TIN VÀ CÁC NGHIÊN CỨU LIÊN QUAN</b> ..... | <b>19</b> |
| 1.1. GIẤU TIN TRONG ẢNH VÀ NGHIÊN CỨU LIÊN QUAN .....  | 19        |
| 1.1.1. Khái niệm .....   | 19        |
| 1.1.2. Phương pháp giấu tin và nghiên cứu liên quan .....  | 21        |
| 1.1.3. Phương pháp đánh giá độ an toàn của một lược đồ giấu tin .....                            | 25        |
| 1.2. PHÁT HIỆN ẢNH GIẤU TIN VÀ CÁC NGHIÊN CỨU LIÊN QUAN .....                                    | 27        |
| 1.2.1. Khái niệm .....   | 27        |
| 1.2.2. Phương pháp phát hiện ảnh có giấu tin .....   | 27        |
| 1.2.3. Nghiên cứu liên quan và hướng phát triển của luận án .....                                | 29        |
| 1.2.3.1. Phương pháp phát hiện mù cho ảnh giấu trên LSB.....                                     | 30        |
| 1.2.3.2. Phương pháp phát hiện ảnh có ràng buộc .....  | 33        |
| 1.3. PHƯƠNG PHÁP THỰC NGHIỆM VÀ ĐÁNH GIÁ.....  | 35        |
| 1.3.1. Tiêu chuẩn đánh giá.....  | 35        |
| 1.3.2. Nguồn dữ liệu ảnh thử nghiệm .....  | 37        |
| 1.3.3. Công cụ hỗ trợ và môi trường thực nghiệm .....  | 39        |
| KẾT LUẬN CHƯƠNG 1 .....  | 39        |
| <b>CHƯƠNG 2. KỸ THUẬT PHÁT HIỆN MÙ CHO ẢNH GIẤU TIN TRÊN LSB</b> .....                           | <b>40</b> |
| 2.1. KỸ THUẬT PHÁT HIỆN MÙ TRÊN LSB CỦA MIỀN KHÔNG GIAN.....                                     | 40        |
| 2.1.1. Phát hiện bằng phân tích “độ lệch chuẩn” .....  | 40        |
| 2.1.1.1. Phân tích kỹ thuật giấu LSB.....  | 40        |
| 2.1.1.2. Phương pháp phát hiện.....  | 42        |
| 2.1.2. Phát hiện bằng thống kê $\chi^2$ một bậc tự do ( $\chi_1^2$ ) .....                       | 46        |
| 2.1.2.1. Phân tích kỹ thuật “độ lệch chuẩn” .....  | 46        |
| 2.1.2.2. Phương pháp phát hiện.....  | 46        |
| 2.1.3. Phát hiện dựa trên phân tích tỉ lệ xám .....  | 50        |
| 2.1.3.1. Phát biểu bài toán .....  | 50        |

|   |           |
|---|-----------|
| 2.1.3.2. Phương pháp giải quyết bài toán.....                               | 51        |
| 2.1.4. Phát hiện bằng phương pháp ước lượng thông tin giấu trên LSB.....    | 60        |
| 2.1.4.1. Phương pháp ước lượng khi có ảnh gốc.....                          | 61        |
| 2.1.4.2. Phương pháp ước lượng không dựa vào ảnh gốc.....                   | 64        |
| 2.2. KỸ THUẬT PHÁT HIỆN MÙ TRÊN LSB CỦA MIỀN TẦN SỐ.....                    | 68        |
| 2.2.1. Phân tích kỹ thuật giấu LSB trên miền tần số.....                    | 68        |
| 2.2.2. Phương pháp phát hiện.....   | 69        |
| 2.3. CÁC KẾT QUẢ THỬ NGHIỆM.....  | 70        |
| 2.3.1. Các kết quả thử nghiệm trên miền không gian.....                     | 70        |
| 2.3.1.1. Thử nghiệm.....  | 70        |
| 2.3.1.2. Nhận xét.....  | 74        |
| 2.3.2. Các kết quả thử nghiệm trên miền tần số.....                         | 75        |
| 2.3.2.1. Thử nghiệm.....  | 75        |
| 2.3.2.2. Nhận xét.....  | 77        |
| KẾT LUẬN CHƯƠNG 2.....  | 77        |
| <b>CHƯƠNG 3. MỘT SỐ KỸ THUẬT PHÁT HIỆN CÓ RÀNG BUỘC.....</b>                | <b>78</b> |
| 3.1. PHÁT HIỆN ẢNH CÓ GIẤU TIN SỬ DỤNG KỸ THUẬT GIẤU HKC.....               | 78        |
| 3.1.1. Tóm lược kỹ thuật giấu HKC.....                                      | 78        |
| 3.1.2. Phương pháp phát hiện và ước lượng thông tin giấu trong ảnh.....     | 79        |
| 3.1.2.1. Phương pháp phát hiện của Kuo và Lin.....                          | 79        |
| 3.1.2.2. Phương pháp phát hiện cải tiến từ phương pháp của Kuo và Lin.....  | 81        |
| 3.1.2.3. Phương pháp phát hiện HKC khác và ước lượng thông tin giấu.....    | 84        |
| 3.1.3. Các kết quả thử nghiệm.....  | 87        |
| 3.1.3.1. Thử nghiệm.....  | 87        |
| 3.1.3.2. Nhận xét.....  | 89        |
| 3.2. PHÁT HIỆN ẢNH CÓ GIẤU TIN SỬ DỤNG KỸ THUẬT GIẤU DIH.....               | 90        |
| 3.2.1. Tóm lược kỹ thuật giấu tin DIH.....                                  | 90        |
| 3.2.2. Phương pháp phát hiện ảnh có giấu tin sử dụng kỹ thuật giấu DIH..... | 91        |
| 3.2.2.1. Phân tích kỹ thuật giấu DIH.....                                   | 91        |
| 3.2.2.2. Phương pháp phát hiện và ước lượng thông tin giấu.....             | 93        |
| 3.2.3. Các kết quả thử nghiệm.....  | 97        |
| 3.2.3.1. Thử nghiệm.....  | 97        |
| 3.2.3.2. Nhận xét.....  | 99        |
| 3.3. PHÁT HIỆN ẢNH CÓ GIẤU TIN SỬ DỤNG KỸ THUẬT GIẤU IWH.....               | 99        |
| 3.3.1. Tóm lược kỹ thuật giấu tin IWH.....                                  | 99        |

|  |            |
|--|------------|
| 3.3.2. Phương pháp phát hiện ảnh có giấu tin sử dụng kỹ thuật giấu IWH.....  | 102        |
| 3.3.2.1. Phân tích kỹ thuật giấu IWH.....                                    | 102        |
| 3.3.2.2. Phương pháp phát hiện và ước lượng thông tin .....                  | 103        |
| 3.3.3. Các kết quả thử nghiệm.....   | 107        |
| 3.3.3.1. Thử nghiệm .....  | 107        |
| 3.3.3.2. Nhận xét .....  | 108        |
| 3.4. PHÁT HIỆN ẢNH CÓ GIẤU TIN SỬ DỤNG KỸ THUẬT GIẤU RVH.....                | 109        |
| 3.4.1. Tóm lược kỹ thuật giấu tin RVH.....                                   | 109        |
| 3.4.2. Phương pháp phát hiện ảnh có giấu tin sử dụng kỹ thuật giấu RVH ..... | 112        |
| 3.4.2.1. Phân tích vấn đề giấu tin RVH.....                                  | 112        |
| 3.4.2.2. Phương pháp phát hiện và ước lượng thông tin .....                  | 115        |
| 3.4.3. Các kết quả thử nghiệm.....   | 122        |
| 3.4.3.1. Thử nghiệm .....  | 122        |
| 3.4.3.2. Nhận xét .....  | 124        |
| KẾT LUẬN CHƯƠNG 3 .....  | 125        |
| <b>KẾT LUẬN CHUNG.....</b>   | <b>126</b> |
| <b>DANH MỤC CÁC CÔNG TRÌNH CÔNG BỐ CỦA TÁC GIẢ.....</b>                      | <b>131</b> |
| <b>TÀI LIỆU THAM KHẢO.....</b>   | <b>132</b> |
| <b>PHỤ LỤC – CHƯƠNG TRÌNH ĐỀ MÔ GIẤU TIN TRONG ẢNH VÀ PHÁT HIỆN</b>          |            |
| <b>    <b>ẢNH CÓ GIẤU TIN.....</b></b>                                       | <b>143</b> |

## DANH MỤC CÁC KÝ HIỆU VÀ TỪ VIẾT TẮT

|       |  |
|-------|--|
| DCT   | Discrete Cosine Transform                                    |
| DFT   | Discrete Fourier Transform                                   |
| DWT   | Discrete Wavelet Transform                                   |
| DIH   | Difference Image Histogram                                   |
| FIR   | Finite Impulse Response                                      |
| HVS   | Human Visual System  |
| HKC   | Kỹ thuật giấu tin của ba tác giả J. Hwang, J. Kim và J. Choi |
| IWT   | Integer Wavelet Transform                                    |
| IDCT  | Inverse Discrete Cosine Transform                            |
| IDWT  | Inverse Discrete wavelet transform                           |
| i.i.d | Independent and Identically Distributed                      |
| JPEG  | Joint Photographic Experts Group                             |
| LLRT  | Logarithm Likelihood Ratio Test                              |
| LSB   | Least Significant Bit  |
| MBNS  | Multiple-Base Notational System                              |
| MOS   | Mean Opinion Score   |
| MSB   | Most Significant Bit   |
| MSE   | Mean Squared Error   |
| NSAS  | Kỹ thuật giấu thuận nghịch NSAS                              |
| Pdf   | Probability Density Function                                 |
| PNG   | Portable Network Graphics                                    |
| PMF   | Probability Mass Function                                    |
| PR    | Pseudo Random  |
| PSNR  | Peak Signal To Noise Ratio                                   |
| PoV   | Pair of Value  |
| QIM   | Quantization Index Modulation                                |
| RS    | Regular /Singular  |
| RVH   | Reversible Vertical Horizontal Technique                     |
| RCM   | Reversible Contrast Mapping                                  |
| SS    | Spread Spectrum  |
| SSIS  | Spread Spectrum Image Steganography                          |

## DANH MỤC CÁC BẢNG

|  |    |
|--|----|
| Bảng 1.1. Bảng phân lớp đối tượng trong tập $\mathcal{E}$ .....  | 36 |
| Bảng 2.1. Giá trị $t_0$ ứng với giá trị $x_0$ theo bảng lập sẵn trong [108] .....  | 45 |
| Bảng 2.2. Phân loại ảnh theo $t_0$ trên tập $\mathcal{C}_{0_1}$ , $\mathcal{S}_{\text{LSB}_{30}}$ , $\mathcal{S}_{\text{LSB}_{50}}$ , $\mathcal{S}_{\text{LSB}_{70}}$ , $\mathcal{S}_{\text{LSB}_{100}}$ .....   | 46 |
| Bảng 2.3. Giá trị $\chi_1^2$ ứng với giá trị $\alpha$ theo bảng lập sẵn trong [108] .....  | 49 |
| Bảng 2.4. Kết quả phân loại ảnh ứng với các giá trị $\chi_1^2$ trong bảng 2.3 .....  | 49 |
| Bảng 2.5. Phân loại ảnh trên $\mathcal{C}_{0_1}$ , $\mathcal{S}_{\text{LSB}_{30}}$ , $\mathcal{S}_{\text{LSB}_{50}}$ , $\mathcal{S}_{\text{LSB}_{70}}$ , $\mathcal{S}_{\text{LSB}_{100}}$ bằng kỹ thuật “Độ lệch chuẩn” và $\chi_1^2$ .....                                      | 50 |
| Bảng 2.6: Kết quả thử nghiệm đánh giá $c_f$ theo (2.14) .....  | 57 |
| Bảng 2.7: Kết quả thử nghiệm đánh giá T theo (2.11) .....  | 59 |
| Bảng 2.8: Kết quả thử nghiệm đánh giá T sau khi ước lượng ảnh “mốc” .....  | 59 |
| Bảng 2.9. Bảng thống kê tần suất xuất hiện của các chữ cái trong văn bản tiếng Anh .....   | 62 |
| Bảng 2.10. Thử nghiệm độ chênh lệch $ c_i^j - s_i^j $ của ảnh có giấu tin và ảnh gốc .....   | 63 |
| Bảng 2.11. Độ sai lệch giữa tần suất của ảnh kiểm tra và ảnh ước lượng làm “mốc” .....   | 65 |
| Bảng 2.12. Kết quả ước lượng xấp xỉ trung bình thông tin giấu trên LSB với tập 10 ảnh ..   | 67 |
| Bảng 2.13. Kết quả ước lượng xấp xỉ theo (2.19) và (2.20) trên tập 10 ảnh chuẩn .....  | 67 |
| Bảng 2.14. Kết quả phân loại ảnh có giấu tin trên LSB trên các tập $\mathcal{C}_0$ , $\mathcal{S}_{\text{LSB}_{30}}$ , $\mathcal{S}_{\text{LSB}_{50}}$ , $\mathcal{S}_{\text{LSB}_{70}}$ , $\mathcal{S}_{\text{LSB}_{100}}$ bằng một số kỹ thuật phát hiện ảnh có giấu tin ..... | 71 |
| Bảng 2.15. Kết quả đánh giá bằng các độ đo P, R, F trên tập ảnh $\mathcal{W}$ gồm 10440 ảnh ( $\mathcal{C}_0$ và $\mathcal{S}_{\text{LSB}_{30}}$ , $\mathcal{S}_{\text{LSB}_{50}}$ , $\mathcal{S}_{\text{LSB}_{70}}$ , $\mathcal{S}_{\text{LSB}_{100}}$ ) .....                  | 71 |
| Bảng 2.16. Kết quả đánh giá bằng các độ đo P, R, F trên tập ảnh $\mathcal{O}$ gồm 4176 ảnh (tập $\mathcal{C}_0$ , $\mathcal{S}_{\text{LSB}_{100}}$ ) .....   | 72 |
| Bảng 2.17. Kết quả ước lượng trên năm tập $\mathcal{C}_0$ , $\mathcal{S}_{\text{LSB}_{30}}$ , $\mathcal{S}_{\text{LSB}_{50}}$ , $\mathcal{S}_{\text{LSB}_{70}}$ , $\mathcal{S}_{\text{LSB}_{100}}$ .....   | 73 |
| Bảng 2.18. Kết quả thời gian thực hiện phân loại trên tập $\mathcal{C}_0$ (2088 ảnh) .....   | 73 |
| Bảng 2.19: Tỷ lệ phân loại ảnh của kỹ thuật “tỉ lệ xám 3” và $\chi_n^2$ [71] với các tập ảnh $\mathcal{J}_0$ , $\mathcal{J}_{25}$ , $\mathcal{J}_{50}$ , $\mathcal{J}_{100}$ .....   | 76 |
| Bảng 2.20. Kết quả đánh giá bằng các độ đo P, R, F trên tập ảnh $\mathcal{J}$ .....  | 76 |
| Bảng 2.21. Thời gian thực hiện trên tập $\mathcal{J}_0$ .....  | 76 |
| Bảng 3.1. Bảng kết quả phân loại trên tập $\mathcal{C}_0$ và $\mathcal{S}_{\text{HKC}_{2500}}$ .....   | 87 |



|   |     |
|---|-----|
| Bảng 3.2. Kết quả đánh giá bằng các độ đo P, R, F trên tập ảnh $\mathcal{V}$ gồm 4176 ảnh ( $\mathcal{C}_0$ và $\mathcal{S}_{\text{HKC}_{2500}}$ ).....                       | 88  |
| Bảng 3.3. Kết quả ước lượng thông tin giấu trên tập $\mathcal{C}_0$ và $\mathcal{S}_{\text{HKC}_{2500}}$ .....  | 88  |
| Bảng 3.4. Bảng kết quả phân loại bằng ba kỹ thuật phát hiện: của Kuo và Lin, của Kuo và Lin cải tiến và kỹ thuật đề xuất mới trên tập $\mathcal{S}_{\text{HKC}_{R100}}$ ..... | 89  |
| Bảng 3.5. Kết quả đánh giá bằng các độ đo P, R, F trên tập ảnh U gồm 4176 ảnh ( $\mathcal{C}_0$ và $\mathcal{S}_{\text{HKC}_{R100}}$ ).....                                   | 89  |
| Bảng 3.6. Sử dụng kỹ thuật phát hiện tổng quát trên miền LSB để phân loại ảnh trên tập $\mathcal{S}_{\text{DIH}_{7168}}$ .....  | 92  |
| Bảng 3.7. Ước lượng thông tin giấu cho ảnh Lena.bmp trước và sau khi giấu tin sử dụng DIH bằng kỹ thuật ước lượng thông tin trên miền LSB: RS, DI, “Trùng khớp”               | 92  |
| Bảng 3.8. Bảng kết quả phân loại ảnh có giấu tin bằng DIH trên tập $\mathcal{C}_0$ và $\mathcal{S}_{\text{DIH}_{6000}}$ .....   | 97  |
| Bảng 3.9. Kết quả ước lượng thông tin giấu trên tập $\mathcal{C}_0$ và $\mathcal{S}_{\text{DIH}_{6000}}$ .....  | 98  |
| Bảng 3.10. Kiểm tra ảnh Lena.bmp trước và sau khi giấu tin sử dụng IWH bằng kỹ thuật phát hiện mù trên miền LSB của các hệ số wavelet.....                                    | 102 |
| Bảng 3.11. Kết quả thử nghiệm ước lượng trên ảnh Lena nhúng 7168 bit.....   | 107 |
| Bảng 3.12. Bảng kết quả phân loại ảnh có giấu tin bằng IWH trên tập $\mathcal{C}_0$ và $\mathcal{S}_{\text{IWH}_{6000}}$ ...  | 107 |
| Bảng 3.13. Kết quả ước lượng thông tin giấu trên tập $\mathcal{C}_0$ và $\mathcal{S}_{\text{IWH}_{6000}}$ .....   | 107 |
| Bảng 3.14. Kiểm tra ảnh stego trên tập $\mathcal{S}_{\text{RVH}_{7168}}$ bằng các kỹ thuật phát hiện tổng quát trên miền LSB.....   | 114 |
| Bảng 3.15. Ước lượng thông tin giấu cho tập $\mathcal{S}_{\text{RVH}_{7168}}$ bằng kỹ thuật RS, DI và “Trùng khớp”.....   | 114 |
| Bảng 3.16. Tỷ lệ phân loại ảnh (gốc và giấu tin) với một số giá trị ngưỡng T.....   | 124 |
| Bảng 3.17. Kết quả ước lượng thông tin giấu trên tập $\mathcal{C}_0$ và $\mathcal{S}_{\text{RVH}_{7500}}$ .....   | 124 |

## DANH MỤC CÁC HÌNH VẼ

|  |     |
|--|-----|
| Hình 1.1: Sơ đồ quá trình giấu tin trong ảnh [84].   | 19  |
| Hình 1.2: Sơ đồ quá trình tách tin trong ảnh.  | 20  |
| Hình 1.3. Minh họa giấu thông tin trong LSB của ảnh cấp xám 8 - bit [84].  | 22  |
| Hình 1.4. Lược đồ quy trình phát hiện ảnh có giấu tin [84]   | 27  |
| Hình 1.5. biểu đồ mật độ xác suất: a) của tập p, b) của tập p sau khi lọc bằng FIR.  | 32  |
| Hình 2.1: Ảnh thử nghiệm cho kỹ thuật “tỉ lệ xám 1”  | 57  |
| Hình 2.2. Tập 10 ảnh chuẩn lấy về từ [107].  | 66  |
| Hình 2.3. Biểu đồ tần suất các hệ số cosine: a) ảnh cover, b) ảnh stego [94].  | 69  |
| Hình 3.1. Biểu đồ tần suất: (a) ảnh gốc, (b) ảnh giấu tin bằng HKC.  | 79  |
| Hình 3.2. Điểm Peak: (a) trước khi giấu tin, (b) sau khi giấu tin  | 80  |
| Hình 3.3. Biểu đồ tần suất của: (a) ảnh gốc, (b) ảnh giấu tin bằng HKC   | 81  |
| Hình 3.4. (a) Ảnh Lena.bmp, (b) thông tin cần giấu là ảnh nhị phân kích cỡ 128 x 56 điểm ảnh, các biểu đồ sai phân: (c) ảnh Lena (gốc), (d) khi dịch chuyển, (e) sau khi giấu tin.                     | 91  |
| Hình 3.5. Tập ảnh thử nghiệm   | 93  |
| Hình 3.6. Biểu đồ tần suất hệ số sai phân của ảnh trước khi giấu tin bằng DIH: a) Airplane.bmp, b) Beer.bmp, c) Elaine.bmp, d) House.bmp, e) Lena.bmp, f) Peppers.bmp, g) Sailboat.bmp, h) Tiffany.bmp | 94  |
| Hình 3.7. Biểu đồ tần suất hệ số sai phân của ảnh sau khi giấu tin bằng DIH: a) Airplane.bmp, b) Beer.bmp, c) Elaine.bmp, d) House.bmp, e) Lena.bmp, f) Peppers.bmp, g) Sailboat.bmp, h) Tiffany.bmp   | 94  |
| Hình 3.8. Kết quả ước lượng độ dài thông tin giấu: a) trên tập ảnh $\mathcal{C}_0$ , b) trên tập $\mathcal{S}_{DIH\_6000}$   | 98  |
| Hình 3.9. Biểu đồ tần suất các hệ số wavelet: (a) Biểu đồ ảnh gốc ban đầu, (b) Biểu đồ sau khi làm rộng một cột tần suất hệ số có giá trị Z [99].  | 100 |
| Hình 3.10. Biểu đồ tần suất hệ số wavelet trên các băng tần cao của: (a) ảnh Lena gốc và ảnh giấu tin với các vị trí ban đầu: (b) T = 3, (c) T = -3, (d) T = 5, (e) T = -6, (f) T = 8.                 | 101 |

|  |     |
|--|-----|
| Hình 3.11. Biểu đồ tần suất hệ số wavelet trên các băng tần cao của các ảnh gốc: a) Airplane.bmp, b) Beer.bmp, c) Elaine.bmp, d) House.bmp, e) Lena.bmp, f) Peppers.bmp, g) Sailboat.bmp, h) Tiffany.bmp .....   | 103 |
| Hình 3.12. Biểu đồ tần suất hệ số wavelet trên các băng tần cao: (a) của ảnh Lena gốc và sau khi giấu tin với các vị trí chọn ban đầu: (b) $T = 2$ , (c) $T = 4$ , (d) $T = 6$ .....   | 104 |
| Hình 3.13. Thử nghiệm ước lượng thông tin trên tập ảnh: a) tập $\mathcal{C}_0$ và b) tập $\mathcal{S}_{IWH\_6000}$ .....   | 108 |
| Hình 3.14. Mô hình tổng quát quá trình nhúng RVH .....   | 109 |
| Hình 3.15. Ảnh Baboon .....  | 113 |
| Hình 3.16. Biểu đồ tần suất của: (a) ảnh cover_Baboon, (b) ảnh stego_Baboon ...  | 113 |
| Hình 3.17. Histogram trên các cột: (a) chẵn, (b) lẻ của ảnh cover_Baboon. Bmp.   | 115 |
| Hình 3.18. Histogram trên các cột: (a) chẵn, (b) lẻ của ảnh stego_Baboon. Bmp...   | 116 |
| Hình 3.19. Sự phân bố của các giá trị $ P_{LSB}(0) - P_{LSB}(1) $ của các điểm ảnh trên các hàng chẵn trong tập: a) $\mathcal{C}_0$ , b) $\mathcal{S}_{RVH\_R25}$ , c) $\mathcal{S}_{RVH\_R50}$ , d) $\mathcal{S}_{RVH\_R75}$ , e) $\mathcal{S}_{RVH\_R100}$ ..... | 123 |

## PHẦN MỞ ĐẦU

### 1. Tính cấp thiết của luận án

“Giấu thông tin” (Steganography<sup>1</sup>) là kỹ thuật liên lạc mật dựa trên hình thức giấu thông tin quan trọng vào đối tượng khác. Từ thời kỳ cổ đại người ta đã sử dụng phương pháp này để liên lạc mật cho nhau. Một ví dụ cổ điển hình về giấu tin [76] (485-525 trước công nguyên) là câu chuyện của một người tên là Histaiæus muốn gửi thông tin quan trọng về “Kế hoạch ủng hộ cuộc nổi dậy chống lại đức vua Ba tư Xerxes” cho nhà nhiếp chính thành phố Miletus bằng cách xăm thông tin lên da đầu người nô lệ tin cậy của mình, cho đến khi tóc mọc dài trở lại ông ta cử người nô lệ đó đến gặp nhà nhiếp chính. Hay một phát minh khác của Pliny T. Elder (23-79 sau công nguyên) về mực “không màu” chính là sữa động vật, khi mực này viết trên giấy để khô khó phát hiện ra, và chỉ khi giấy đó được hơi nóng các vết mực sẽ chuyển sang nâu. Vào thời kỳ phục hưng, năm 1518 Johannes Trithemius viết cuốn sách về mã hóa “Polygraphia”. Trong cuốn sách này người ta thấy xuất hiện đầu tiên thuật ngữ “Steganographia”, đây là một từ ghép bắt nguồn từ ngôn ngữ Hy Lạp *steganos* nghĩa là bao bọc “cover” và *graphia* nghĩa là *bản viết* “writing” [27].

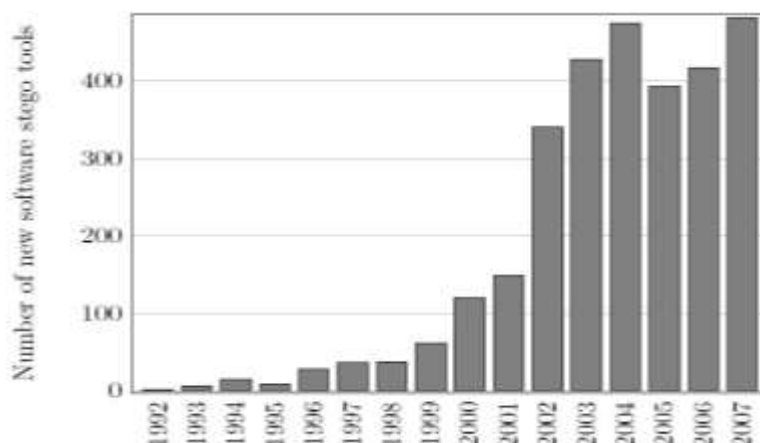
Trải qua nhiều thời kỳ biến động của xã hội loài người, ngày nay khi mà kỹ thuật số bùng nổ, con người cũng “số hoá” lĩnh vực giấu tin phục vụ cho cuộc sống hiện đại. Do tính ưu việt của các kỹ thuật giấu tin là “vô hình” nên nó trở thành công cụ hữu ích cho một số tổ chức trao đổi thông tin quan trọng trong môi trường truyền thông công cộng. Vì vậy giấu tin mật phát triển một cách nhanh chóng và ngày càng tinh xảo hơn với một lượng lớn công trình giấu tin được công bố thường niên (chưa kể đến số kỹ thuật giấu không công bố công khai) như thống kê trong biểu đồ hình 1 giai đoạn từ năm 1992 đến 2007 của Jessica Fridrich [32].

Giấu tin có một ưu điểm mà mật mã học (Cryptography) còn hạn chế đó là có thể “bảo vệ được bản quyền số, hay khi giữa các đối tượng liên lạc mật với nhau trên các kênh thông tin công cộng mà ít bị nghi ngờ”. Lý do vì bản quyền số đã mã

---

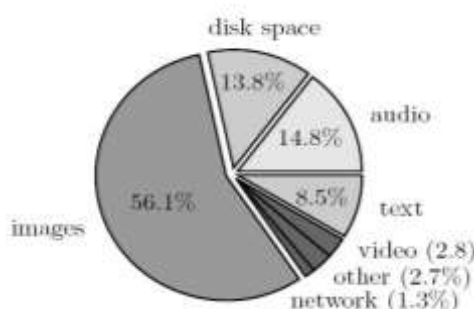
<sup>1</sup> Thuật ngữ *Steganography* được tạm dịch thành “Giấu tin” và được sử dụng trong toàn bộ luận án này

hóa sau khi được giải mã thì khó có thể giữ được bản quyền, hay thông tin mật cần trao đổi giữa các bên, sau khi được mã hóa sẽ làm cho người khác biết rõ là các bên có trao đổi thông tin mật nào đó cho nhau. Giấu tin trong dữ liệu đa phương tiện chính là những “bỏ khuyết” cho các vấn đề trên của mật mã học.



Hình 1. Kỹ thuật giấu tin công bố trong giai đoạn 1992 – 2007[32]

Về nguyên lý, giấu tin trong dữ liệu video, dữ liệu âm thanh hay trong dữ liệu ảnh số không khác gì nhiều. Tuy nhiên, do giấu tin trong ảnh dễ thực hiện hơn, giấu được nhiều thông tin hơn, và ảnh là đối tượng được sử dụng khá phổ biến trên Internet hiện nay, nên kỹ thuật giấu tin trong ảnh chiếm tỉ lệ nhiều nhất trong các loại dữ liệu đa phương tiện (hình 2).



Hình 2. Tỉ lệ phương tiện được lựa chọn để giấu tin năm 2008 [32]

Vậy giấu tin trong ảnh là gì ? Tại sao nó lại phát triển nhanh và sôi động như vậy ? Theo [18, 27], giấu thông tin là kỹ thuật “nhúng” một lượng thông tin vào dữ liệu ảnh số sao cho đảm bảo các yêu cầu sau:

1/. Không thể phát hiện (undetectability) thông tin giấu trong ảnh gốc bằng cảm nhận của con người.

2/. Không thể phân biệt được (undistinguishable) đâu là ảnh gốc và đâu là ảnh có giấu tin bằng cảm nhận của con người.

3/. Lượng thông tin giấu lớn nhất có thể (steganographic capacity) trong gốc sao cho không vi phạm yêu cầu 1/ và yêu cầu 2/ nêu trên. Ngoài ra, việc giấu thông tin trong ảnh còn đem lại khả năng tiết kiệm bộ nhớ và thời gian truyền tin đáng kể. Ví dụ: Giả sử một ảnh xám 8 – bit có kích cỡ 4×6 cm tương ứng với 630×945 pixel (tương đương 595350 pixel). Nếu mỗi pixel giấu được một bit thông tin, thì 595350 pixel có thể giấu lượng thông tin lấp đầy 19 trang giấy A4 (trung bình mỗi trang A4 chứa được 75 ký tự × 50 dòng).

Thông tin có thể được giấu trên miền không gian hoặc trên các hệ số biến đổi của ảnh như biến đổi tần số cosine rời rạc, wavelet rời rạc, fourier rời rạc hay biến đổi sai phân (difference image).

Kỹ thuật giấu tin trong ảnh đa số là phương pháp giấu trên bit có ít ý nghĩa nhất LSB (Least Significant Bit) của điểm ảnh hoặc của các hệ số biến đổi, vì thay đổi trên bit LSB ít ảnh hưởng đến chất lượng ảnh theo khả năng cảm nhận của con người [16, 17, 19, 50, 51, 53 - 55, 65, 67, 69, 75, 77, 91, 100]. Ngoài ra còn có một số phương pháp giấu khác theo cách thức có sự thay đổi nhỏ trên ảnh như phương pháp giấu theo hình thức chèn nhiễu – kỹ thuật giấu tin SS (Spread Spectrum) [3, 4, 26, 60], phương pháp giấu tin theo hình thức điều chỉnh hệ số lượng tử QIM (Quantization Index Modulation) [5, 23, 42, 65, 79], hay một số kỹ thuật giấu đặc biệt khác: MBNS [101], RCM [25], RVH [45],...

Giống như trong Mật mã học, Thám mã (Cryptanalysis) là kỹ thuật đối lập nhưng song song tồn tại và phát triển cùng với sự phát triển của kỹ thuật Mật mã, nhằm giải mã các “bản mã” thu nhận được để hiểu rõ nội dung ban đầu của bản mã,

thì phát hiện ảnh có giấu tin (image steganalysis<sup>2</sup>) là kỹ thuật đối lập với kỹ thuật giấu tin nhằm dò tìm ảnh số nào đó có giấu thông tin hay không.

Việc nghiên cứu phát hiện ảnh giấu tin ngoài ý nghĩa khoa học còn có hai ý nghĩa thực tiễn, đó là: Thứ nhất, nhằm phục vụ đắc lực cho an ninh quốc phòng của mỗi quốc gia; Thứ hai, nhằm nâng cấp và thúc đẩy sự phát triển của kỹ thuật giấu tin trong ảnh. Chính vì vậy, ở các nước, nhất là các nước có nền công nghiệp phát triển như: Mỹ, Anh, Đức, Israel, Trung Quốc, Hàn Quốc, Nhật Bản ... đã đầu tư rất nhiều kinh phí cho việc nghiên cứu này. Tại Việt Nam, cũng đã có một số cơ quan đơn vị nghiên cứu về giấu tin trong ảnh và phát hiện ảnh có giấu tin như: Tổng Cục an ninh I – Bộ Công An, Viện Công Nghệ Thông tin – Viện khoa học Việt Nam, trường Đại học bách khoa Hà Nội, trường Đại học Khoa học Tự nhiên Thành phố Hồ Chí Minh... nhưng vẫn còn rời rạc và chưa được đầu tư đúng mức.

Với hai mục đích nêu trên dẫn đến hai hướng nghiên cứu khác nhau : Hướng thứ nhất, cố gắng xây dựng thuật toán phát hiện mù (blind steganalysis) cho ảnh có giấu tin sử dụng kỹ thuật giấu bất kỳ; Hướng thứ hai, dựa vào kỹ thuật giấu tin nào đó đã biết, có thể xây dựng được thuật toán phát hiện phù hợp (phát hiện có ràng buộc – constraint steganalysis).

Đã có nhiều công trình công bố nghiên cứu trên thế giới thành công theo hai hướng này :

- Với kỹ thuật phát hiện mù cho ảnh có giấu tin trên LSB của miền không gian có các công trình [31, 38, 84, 95, 102] và miền tần số có công trình [71], kỹ thuật phát hiện mù cho ảnh giấu tin sử dụng kỹ thuật giấu SS có công trình [83], kỹ thuật giấu QIM có các công trình [59, 81, 82] hay phát hiện mù cho ảnh JPEG có giấu tin [66].
- Với kỹ thuật phát hiện có ràng buộc cho ảnh có giấu tin sử dụng một số kỹ thuật giấu đã biết, như các công trình: [36] (tấn công kỹ thuật giấu OutGuess), [33] (tấn công kỹ thuật giấu F5), [46] (tấn công kỹ thuật giấu

---

<sup>2</sup> Thuật ngữ *image steganalysis* được tạm dịch là “phát hiện ảnh giấu tin”

HKC), [24] (tấn công kỹ thuật giấu RCM), [14] (tấn công kỹ thuật giấu tin MBNS).

Tuy nhiên, các kỹ thuật giấu tin ra đời sau ngày càng tinh xảo hơn đòi hỏi các nhà phân tích ảnh có giấu tin không ngừng tìm ra phương pháp phát hiện phù hợp bắt kịp với xu hướng phát triển của kỹ thuật giấu thông tin. Đặc biệt với tốc độ phát triển nhanh chóng của Internet ngày nay thì nhu cầu trao đổi thông tin bằng ảnh ngày càng lớn mạnh, do đó để đảm bảo an toàn an ninh, quốc phòng hay hỗ trợ nâng cấp, cải tiến kỹ thuật giấu nào đó an toàn hơn đang là bài toán cấp thiết đặt ra cho các nhà nghiên cứu trong lĩnh vực an toàn thông tin ở nước ta hiện nay.

## **2. Mục tiêu và phạm vi nghiên cứu**

Từ phân tích nêu trên, luận án này tập trung nghiên cứu cải tiến và đề xuất một số kỹ thuật phát hiện ảnh có giấu tin theo hai hướng chính:

- Thứ nhất, đưa ra một số kỹ thuật phát hiện mù cho ảnh có giấu tin trên LSB của miền không gian và miền tần số. Từ việc khảo sát, phân tích kỹ thuật giấu LSB và một số kỹ thuật phát hiện của tác giả khác luận án đưa ra phương pháp phát hiện khác cho kết quả phân loại tương đương hoặc tốt hơn trong trường hợp nào đó so với các kỹ thuật phát hiện khác.
- Thứ hai, đưa ra một số kỹ thuật phát hiện có ràng buộc cho ảnh có giấu tin với kỹ thuật giấu biết trước. Kỹ thuật giấu biết trước thường là trường hợp riêng của kỹ thuật giấu LSB, nó cho phép giấu với lượng thông tin giấu thấp, vì vậy nếu quy về bài toán phát hiện mù sẽ cho kết quả phát hiện không cao, trong các trường hợp riêng này thường sẽ cố gắng tìm ra phương pháp phát hiện tối ưu hơn các phương pháp phát hiện mù.

Đối tượng ảnh nghiên cứu là các ảnh dạng BITMAP vì hầu hết các ảnh trong máy tính, các ảnh chụp từ máy ảnh kỹ thuật số hoặc các ảnh từ các trang web là lưu dưới dạng này (như các định dạng: jpg, gif, png, tif, psp, bmp, ...), còn ảnh dạng vector (như các định dạng: pdf, eps, ai, cdr, svg, dwg, ...) không nằm trong phạm vi nghiên cứu của luận án này.



### 3. Những đóng góp của luận án

Những đóng góp chính của luận án là đưa ra kỹ thuật phát hiện ảnh có giấu tin theo hai bài toán sau:

Bài toán 1: Kỹ thuật phát hiện mù cho ảnh có giấu tin trên LSB của miền không gian (miền tần số) với các kỹ thuật đề xuất sau:

- Đề xuất ba kỹ thuật phát hiện mù cho ảnh có giấu tin trên LSB của miền không gian bằng: phương pháp phân tích độ lệch chuẩn, phương pháp thống kê  $\chi^2$  một bậc tự do ( $\chi_1^2$ ), phương pháp phân tích tỉ lệ xám.
- Đề xuất một kỹ thuật phát hiện mù cho ảnh giấu tin trên LSB của miền tần số bằng phân tích tỉ lệ xám.
- Đề xuất phương pháp phát hiện mù bằng cách ước lượng thông tin giấu trên LSB của miền không gian dựa trên lý thuyết trùng khớp.

Bài toán 2: Kỹ thuật phát hiện có ràng buộc cho ảnh có giấu tin sử dụng kỹ thuật giấu đã biết gồm:

- Kỹ thuật giấu thuận nghịch IWH trên hệ số wavelet.
- Kỹ thuật giấu thuận nghịch DIH trên hệ số sai phân.
- Kỹ thuật giấu HKC trên miền không gian.
- Kỹ thuật giấu RVH với hai pha ngang dọc.

Tiến hành thực nghiệm trên những bộ dữ liệu có số lượng ảnh lớn để so sánh kỹ thuật mới đề xuất với các kỹ thuật khác đã biết. Tập ảnh sử dụng để thử nghiệm gồm một phần ảnh tải về từ các thư viện ảnh trực tuyến của trường đại học Washington [103], đại học Southern California [107] và một phần được tạo ra từ máy ảnh kỹ thuật số và điện thoại di động.

### 4. Tổ chức luận án

Luận án gồm ba chương, mỗi chương đều có phần giới thiệu và phần kết luận chương. **Chương 1** giới thiệu tổng quan về giấu tin trong ảnh, phát hiện ảnh có giấu tin và các nghiên cứu liên quan. Ngoài ra, chương này còn nêu ra phương pháp đánh giá các kỹ thuật phát hiện ảnh có giấu tin theo chuẩn đánh giá độ chính xác (Precision), độ bao phủ (Recall), độ trung bình điều hòa (F-measure) và nguồn dữ liệu ảnh sử dụng để thử nghiệm.

**Chương 2** đề xuất một số kỹ thuật phát hiện mù cho ảnh có giấu tin trên LSB gồm các kỹ thuật phát hiện: “độ lệch chuẩn”, “ $\chi_1^2$ ”, “tỉ lệ xám” và phát hiện bằng phương pháp ước lượng thông tin giấu trong sử dụng lý thuyết “trùng khớp”. Từ đó đưa ra kết quả so sánh giữa các kỹ thuật đề xuất và một số phương pháp phát hiện mù khác:  $\chi^2$  với n bậc tự do của A. Westfeld [15], LLRT của K. Sullivan [80] và kỹ thuật ước lượng: RS của Jessica Fridrich và cộng sự [31], DI của T. Zhang và X. Ping [102] cho thấy kết quả tương đương và hiệu quả hơn ở một số trường hợp.

**Chương 3** đề xuất bốn kỹ thuật phát hiện có ràng buộc cho ảnh có giấu tin sử dụng một số kỹ thuật giấu tin đã biết: DIH, HKC, IWH và RVH. Các kết quả thử nghiệm cho thấy độ tin cậy của kỹ thuật phát hiện đề xuất.

Phần cuối cùng là phần **kết luận chung** và **phụ lục**.

**Phụ lục** chương trình đề mô với hai mô đun chính: Mô đun giấu tin và mô đun phát hiện ảnh giấu tin. Mỗi mô đun gồm các chức năng phục vụ các thử nghiệm trong luận án.

# Chương 1. GIẤU TIN TRONG ẢNH, PHÁT HIỆN ẢNH CÓ GIẤU TIN VÀ CÁC NGHIÊN CỨU LIÊN QUAN

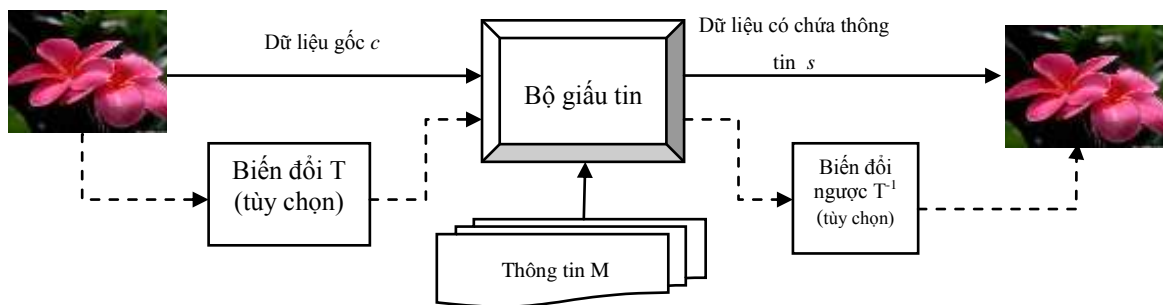
Trong chương này trình bày tổng quan về kỹ thuật giấu tin trong ảnh, các phương pháp giấu tin thường sử dụng trong thời gian gần đây, kỹ thuật phát hiện ảnh có giấu tin và các nghiên cứu liên quan. Từ đó đưa ra phương pháp phát hiện ảnh có giấu tin đề xuất trong chương 2 và 3. Ngoài ra chương này còn giới thiệu phương pháp thử nghiệm, đánh giá và nguồn dữ liệu ảnh thử nghiệm cho các kỹ thuật phát hiện đề xuất trong các chương tiếp theo.

## 1.1. GIẤU TIN TRONG ẢNH VÀ NGHIÊN CỨU LIÊN QUAN

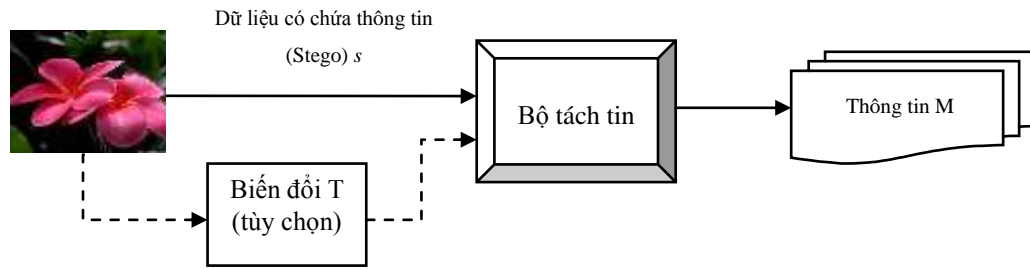
### 1.1.1. Khái niệm

Giấu tin trong ảnh (image steganography) là kỹ thuật lợi dụng một số thông tin dư thừa của dữ liệu ảnh gốc (cover image) để giấu (hoặc nhúng) thông tin vào đó. Kỹ thuật giấu này phải đảm bảo chỉ người gửi (giấu) và người nhận (tách) biết thông tin đã giấu, còn những người khác khó có thể cảm nhận được sự tồn tại của thông tin đã giấu trong ảnh [18, 27, 32].

Giấu tin trong ảnh gồm hai giai đoạn: nhúng thông tin vào ảnh gốc và tách thông tin đã giấu. Để tăng cường độ an toàn cho thông tin đem giấu, thường thì trước khi giấu thông tin có thể được mã hóa bằng kỹ thuật mã hóa nào đó [27, 45, 74]. Trong quá trình tách thông tin, dữ liệu gốc có thể tham gia hoặc không. Các kỹ thuật giấu tin tốt thường không cần dữ liệu gốc để tách thông tin đã giấu.



Hình 1.1: Sơ đồ quá trình giấu tin trong ảnh [84].



Hình 1.2: Sơ đồ quá trình tách tin trong ảnh.

Hình 1.1 và 1.2 là sơ đồ tổng quát của quá trình giấu tin và tách tin trong ảnh, trong đó phép biến đổi  $T$  và  $T^{-1}$  là các phép biến đổi tần số cosine, wavelet, fourier rời rạc hoặc biến đổi sai phân (image difference). Dưới đây là tóm lược một số phép biến đổi sử dụng trong luận án này:

- Biến đổi cosine rời rạc được thực hiện theo chuẩn nén ảnh JPEG, miền dữ liệu pixel của ảnh được chia thành các miền nhỏ (thường là kích cỡ  $8 \times 8$  hoặc  $16 \times 16$  pixel) sử dụng phép biến cosine rời rạc được các hệ số cosine [43], thông tin thường được giấu vào các hệ số cosine có giá trị lớn nhất hoặc nằm ở miền tần số giữa như các kỹ thuật giấu [3, 7, 23, 25, 69, 70, 92, 94, 104].
- Biến đổi wavelet rời rạc, sử dụng phép biến đổi wavelet rời rạc biến đổi miền dữ liệu pixel thành bốn băng tần mới LL, LH, HL, HH [72, 99]. Các giá trị trên bốn băng tần này gọi là các hệ số wavelet. Theo nhận định của những nhà giấu tin thì khi có thay đổi nhỏ các hệ số wavelet trên hai băng tần cao LH và HL (một số kỹ thuật giấu sử dụng cả băng tần HH) sẽ ít ảnh hưởng đến chất lượng trực quan của ảnh ban đầu như các kỹ thuật giấu [4, 5, 6, 42, 73, 91, 99]. Còn băng tần LL không hay sử dụng để giấu tin vì nó chính là nội dung thu nhỏ của ảnh, khi giấu vào băng tần này sẽ ảnh hưởng đến chất lượng của ảnh ban đầu.
- Biến đổi sai phân (image difference), giả sử dữ liệu ảnh nào đó, kích thước  $m \times n$  pixel, được biểu diễn dưới dạng vector  $X = \{x_{ij}, i=0, \dots, m-1, j=0, \dots, n-1\}$ , miền giá trị pixel của ảnh sẽ được biến đổi sang miền giá trị sai phân được vector các hệ số sai phân  $D = \{d_{ij}\}$  trong đó  $d_{ij} =$

$x_{i,2j+1} - x_{i,2j}$  với  $0 \leq i \leq m - 1, 0 \leq j \leq n/2 - 1$  hoặc  $d_{ij} = x_{i,j-1} - x_{i,j}$  với  $0 \leq i \leq m - 1, 0 \leq j \leq n - 2$ . Thông tin thường được giấu trên LSB của các hệ số này như các kỹ thuật [48, 49, 52, 53, 90, 97].

### 1.1.2. Phương pháp giấu tin và nghiên cứu liên quan

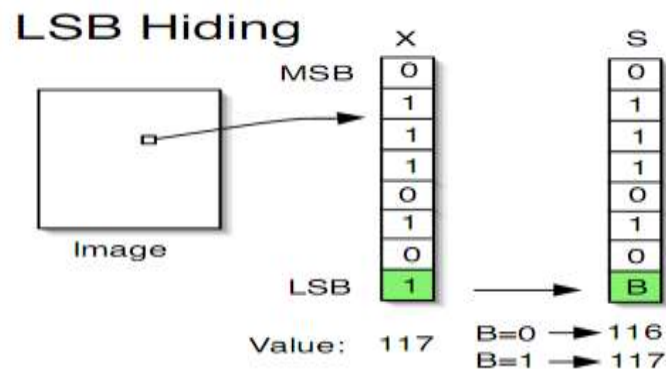
Kỹ thuật giấu tin trong ảnh ra đời dựa trên sự phát triển ưu việt của kỹ thuật thủy vân số (Watermarking), phương pháp thủy vân ảnh số đầu tiên là phương pháp thủy vân trên LSB của ảnh hay còn gọi là phương pháp thay thế LSB (LSB replacement – LSB hiding) và nó cũng trở thành phương pháp giấu tin đầu tiên trong ảnh [75].

Phương pháp giấu tin trên LSB là phương pháp thay thế các bit thông tin vào bit LSB của điểm ảnh. Trong một điểm ảnh của ảnh 8-bit cấp độ xám có thể biểu diễn dưới dạng chuỗi nhị phân 8 bit (giả sử điểm ảnh P có giá trị 236 có thể biểu diễn thành chuỗi nhị phân 8 bit là “11101100”) thì 7 bit liên tiếp đầu tiên (là chuỗi bit “1110110”) gọi là các bit MSBs (Most Significant Bit) có ý nghĩa quan trọng nhất đối với điểm ảnh, còn bit cuối cùng (bit “0”) gọi là bit LSB vì có ảnh hưởng ít nhất đến sự thể hiện của điểm ảnh. Do vậy, việc thay đổi giá trị của bit LSB (từ “0” sang “1” hay từ “1” sang “0”) không làm ảnh hưởng nhiều đến chất lượng trực quan của ảnh.

Kỹ thuật giấu tin trên LSB vẫn còn được ưa chuộng cho đến ngày nay ở chỗ nó rất đơn giản và có khả năng giấu được nhiều thông tin. Mỗi điểm ảnh có thể nhúng được một bit thông tin, do đó tỉ lệ nhúng lớn nhất là một bit thông tin trên một điểm ảnh (hay độ dài bit thông tin có thể nhúng bằng số điểm ảnh của ảnh).

Để đơn giản, giả sử ảnh gốc đầu vào để giấu tin là ảnh xám 8 – bit kích cỡ  $m \times n$  điểm ảnh, dữ liệu ảnh được biểu diễn dưới dạng vector  $X^{m \times n} = \{x_{ij}, i=1, \dots, m, j=1, \dots, n, x_{ij} \in \{0, \dots, 255\}\}$ . Sau khi giấu chuỗi bit thông tin  $B^l = \{b_i, i = 1, \dots, l, b_i \in \{0,1\}\}$  vào ảnh bằng cách thay thế từng bit  $b_i \in B$  vào từng bit LSB của  $x_{ij}$  theo thứ tự nào đó ta nhận được ảnh có giấu tin với vector  $S^{m \times n} = \{s_{ij}, i=1, \dots, m, j=1, \dots,$

$n, s_{ij} \in \{0, \dots, 255\}$  tương ứng. Khi đó LSB của điểm ảnh được giấu tin theo mô tả như hình 1.3 (giấu trên điểm ảnh có giá trị bằng 117).



Hình 1.3. Minh họa giấu thông tin trong LSB của ảnh cấp xám 8 - bit [84].

Việc áp dụng hàm giấu và tách thông tin có thể thực hiện tương tự trên ảnh 24 - bit màu với 3 kênh màu R, G, B (mỗi kênh 8 – bit), khi đó việc giấu tin thường thực hiện trên kênh màu B (được cho là ít ảnh hưởng đến hệ thống cảm nhận của mắt người [27]) như quá trình giấu tin trên ảnh 8 – bit cấp độ màu.

Để đảm bảo ảnh sau khi đã giấu tin bằng kỹ thuật giấu LSB trên miền không gian không bị phá vỡ bằng một số phép tấn công hình học như xoay, nén, co, giãn, ... người ta đề xuất một số phương pháp giấu cải tiến LSB khác trên miền tần số: cosine [3, 7, 23, 25, 94, 104], wavelet [91, 99]. Một số khác còn giấu trên LSB của các hệ số sai phân [49, 53, 90, 97].

Bit LSB của điểm ảnh hay của hệ số biến đổi được chọn để giấu thông tin có thể chọn theo *thứ tự tuần tự* (quét raster) (như kỹ thuật giấu EzStego [105], Jstego [104 ], DE [91], ...) hoặc theo *thứ tự ngẫu nhiên* dựa trên một bộ chọn vị trí giả ngẫu nhiên PR (Pseudo Random) (như kỹ thuật giấu OutGuess [71], F5 [94], Hide and Seek [69], ...). Ngoài ra còn có hai trường đặc biệt giấu trên LSB đó là: phương pháp tăng giảm LSB, phương pháp đồng chẵn lẻ.

*Phương pháp tăng giảm LSB ( $\pm 1$  embedding)*, bit thông tin sẽ được so sánh với bit LSB của điểm ảnh được chọn (việc chọn điểm ảnh có thể là tuần tự hoặc ngẫu nhiên theo bộ chọn PR). Nếu bit thông tin cùng giá trị với bit LSB của điểm

ảnh cần giấu thì mặc định sẽ giấu một bit thông tin vào điểm ảnh này, ngược lại điểm ảnh cần giấu sẽ tăng hoặc giảm đi 1 để LSB của nó đồng giá trị với bit thông tin. Một số kỹ thuật giấu sử dụng phương pháp giấu này như [78, 49],...

*Phương pháp đồng chẵn lẻ*, chia miền không gian ảnh ra thành nhiều khối bằng nhau kích thước  $k \times t$ , bit thông tin sẽ được giấu vào từng khối theo quy tắc: số bit LSB có giá trị “1” của khối phải đồng tính chẵn lẻ với bit được giấu, tức là số bit “1” của một khối LSB là lẻ nếu bit thông tin cần giấu là “1”, ngược lại là chẵn nếu bit cần giấu là “0”. Trong trường hợp không trùng hợp, ta phải thay đổi giá trị LSB của khối đó để đảm bảo đồng tính chẵn lẻ với bit thông tin. Trường hợp đặc biệt, nếu kích thước mỗi khối dùng để giấu tin là  $1 \times 1$ , thì nó trở thành trường hợp giấu thay thế LSB tổng quát. Kỹ thuật giấu sử dụng phương pháp giấu này như [78], chỉ áp dụng cho miền không gian không áp dụng được cho miền tần số.

Có thể có nhiều phương pháp giấu LSB khác nhau không tuân theo bốn phương pháp đã nêu ở trên, đó là các phương pháp kết hợp với một trong bốn phương pháp trên (*phương pháp tuần tự*, *phương pháp ngẫu nhiên*, *phương pháp tăng giảm*, *phương pháp đồng chẵn lẻ*) cùng với một số thao tác nào đó nhằm nâng cao hiệu quả an toàn cho thông tin được giấu.

Ngoài phương pháp giấu trên LSB còn có một số phương pháp giấu tin khác theo hình thức *chèn nhiều SS* hay *điều chỉnh hệ số lượng tử QIM* như sau:

*Kỹ thuật giấu tin theo hình thức chèn nhiều SS*: Dữ liệu đem giấu sẽ được điều biến thành một chuỗi tín hiệu mang thông tin theo một hệ số bền vững  $\alpha$ , sau đó được chèn vào dữ liệu ảnh gốc. Với cách thức giấu tin theo kiểu SS đã có nhiều phương pháp được đề xuất [3, 4, 26, 27, 32, 60]. Điển hình như phương pháp của J. Cox [26], ảnh gốc sẽ được biến đổi Cosine và chọn ra một lượng hệ số DCT  $x_k$  ở miền tần số giữa có giá trị lớn nhất bằng độ dài tín hiệu thông tin cần giấu, các tín hiệu thông tin  $d_k$  trong chuỗi thông tin sẽ được chèn vào các hệ số  $x_k$  này theo một trong ba công thức sau:  $s_k = x_k + \alpha d_k$ ,  $s_k = x_k + (\alpha x_k) d_k = x_k (1 + \alpha d_k)$  hoặc  $s_k = x_k e^{\alpha d_k}$ . Theo J.Cox, các biểu thức hiệu chỉnh này cho phép giấu thông tin bền vững trong ảnh trước các tấn công nhiễu và một số phép biến đổi hình học.

*Kỹ thuật giấu tin điều chỉnh hệ số lượng tử QIM*: là một phương pháp giấu khá phổ biến mặc dù kỹ thuật giấu hơi phức tạp và khả năng giấu thấp hơn kỹ thuật giấu LSB, nhưng cũng giống như kỹ thuật giấu SS, QIM làm cho thông tin có thể bền vững trước các tấn công hình học và nhiễu. Giả sử coi dữ liệu của ảnh gốc và ảnh có giấu tin là các tín hiệu ký hiệu lần lượt là  $\{x_n\}_{n=1}^N$  và  $\{s_n\}_{n=1}^N$ ,  $M$  là chuỗi thông tin cần giấu, khi đó ta có  $S(X, M) = q_M(X)$ . Tín hiệu của ảnh có giấu tin bao gồm các giá trị trong tập lượng tử đầu ra, do đó sẽ hạn chế cho trường hợp nén dữ liệu, sẽ làm mất thông tin đã giấu. Để có thể cung cấp một tín hiệu ảnh giấu tin bao phủ tất cả các giá trị của tín hiệu gốc, việc lượng tử sẽ được dịch chuyển theo một mức thay đổi nhỏ  $D$  bằng biểu thức  $S(X, M) = q(X + D(M)) - D(M)$  với  $q_M$  là hàm lượng tử,  $D$  là hàm điều chỉnh lượng tử. Có nhiều phương pháp giấu tin đề xuất theo hình thức giấu này [5, 23, 42, 65, 79].

Thời gian gần đây do đặc thù của một số lĩnh vực: y học, quân sự, nghiên cứu năng lượng hoặc hệ thống thông tin vệ tinh, ... đòi hỏi yêu cầu sau khi tách thông tin chúng ta có thể khôi phục lại ảnh gốc ban đầu. Vì vậy kỹ thuật giấu tin thuận nghịch ra đời. Năm 1999, Honsinger và các cộng sự đề xuất kỹ thuật giấu thuận nghịch đầu tiên [39], mở ra một hướng mới trong lĩnh vực giấu tin. Tiếp đó một loạt các kỹ thuật giấu tin thuận nghịch khác được công bố [21, 24, 25, 35, 41, 45, 48, 49, 52, 53, 58, 90, 91, 93, 98, 99]. Sau đây giới thiệu sơ lược một số kỹ thuật giấu tiêu biểu.

Kỹ thuật mở rộng sai phân DE (Difference Expansion) do Tian đưa ra (2002) [90], đây là kỹ giấu tin dựa trên mở rộng hệ số sai phân của điểm ảnh, dữ liệu ảnh được tính sai phân theo biểu thức (1.1), thông tin được giấu trên LSB của các hệ số sai phân sau khi được mở rộng. Sau đó tác giả đề xuất tiếp phương pháp mở rộng trên các hệ số wavelet để giấu tin [91]. Đến năm 2008, Shaowei Weng và các đồng nghiệp đưa ra kỹ thuật DE cải tiến [93] bằng cách thêm vào hàm nén – giãn trong quá trình giấu tin sử dụng DE nhằm giảm nhiễu xảy ra (theo đánh giá bằng PSNR) của kỹ thuật giấu thuận nghịch DE.



Năm 2003, Ni và cộng sự đề xuất kỹ thuật giấu thuận nghịch dựa trên dịch chuyển biểu đồ tần suất gọi là NSAS [62]. Tiếp đó một loạt các kỹ thuật giấu thuận nghịch dựa phương pháp này ra đời: kỹ thuật DIH [49] (2004) (dịch chuyển biểu đồ tần suất hệ số sai phân), kỹ thuật HKC [41] (cải tiến kỹ thuật giấu NSAS), kỹ thuật IWH [99] (2006) (dựa trên dịch chuyển biểu đồ tần suất hệ số wavelet nguyên), kỹ thuật RL (2008) [98] là kỹ thuật giấu thuận cho ảnh nhị phân dựa trên dịch chuyển tần suất của các loạt đen trong ảnh.

Một số kỹ thuật giấu thuận nghịch khác không dựa trên biểu đồ tần suất như: Kỹ thuật giấu MBNS (Multiple-Base Notational System) [101]: dữ liệu cần giấu được chuyển đổi thành các hệ số nhỏ hơn theo phương pháp phân tích nhân tử thành đa thức, các điểm ảnh sẽ được điều chỉnh để lưu trữ các hệ số này; kỹ thuật giấu RCM dựa trên hiệu chỉnh LSB của ảnh theo bản đồ màu tương phản [25]; Kỹ thuật giấu hai pha ngang dọc RVH [45], chuỗi thông tin giấu  $M$  được chia thành hai chuỗi con bằng nhau  $M_1$  và  $M_2$ , sau đó được giấu lần lượt vào hai pha: Pha giấu ngang, thực hiện giấu trên các cột lẻ của ma trận ảnh; Pha giấu dọc, thực hiện giấu trên các hàng chẵn của ma trận ảnh.

### 1.1.3. Phương pháp đánh giá độ an toàn của một lược đồ giấu tin

Khi một kỹ thuật giấu tin được đề xuất, từ đòi hỏi “khó có thể cảm nhận bằng mắt thường” hay “không thể phát hiện bằng phương pháp thống kê” Cachin đã đưa ra một khái niệm về giấu tin an toàn [15].

Trước tiên, chúng ta cần đưa ra một vài ký hiệu sẽ được sử dụng xuyên suốt luận án này. Đặt  $\mathcal{C}$  ký hiệu là tập tất cả các ảnh gốc  $C$ ,  $\mathcal{M}$  là tập các thông tin mật  $M$ ,  $\mathcal{K}$  là tập các khóa  $K$  giấu tin,  $\mathcal{S}$  là tập tất cả các ảnh stego  $S$ . Một lược đồ giấu tin (thuật toán) là một cặp  $(S_E, S_X)$ , với  $S_E: \mathcal{C} \times \mathcal{M} \times \mathcal{K} \rightarrow \mathcal{S}$  là hàm nhúng thông tin và  $S_X: \mathcal{S} \times \mathcal{K} \rightarrow \mathcal{M}$  là hàm tách thông tin. Hàm nhúng  $S_E$  tạo ra một đối tượng  $S \in \mathcal{S}$  từ mỗi  $C \in \mathcal{C}$ ,  $M \in \mathcal{M}$  và  $K \in \mathcal{K}$ , tương tự hàm tách  $S_X$  tách thông tin  $M$  từ  $S$  bằng khóa  $K$ .

Giả sử  $P_C$  hàm phân bố xác suất của  $C \in \mathcal{C}$ . Nếu khóa  $K \in \mathcal{K}$  và  $M \in \mathcal{M}$  được chọn ngẫu nhiên thì lược đồ giấu tin ( $S_E, S_X$ ) cùng với hàm phân bố xác suất  $P_C$  sẽ được hàm phân bố xác suất  $P_S$  tương ứng của  $S \in \mathcal{S}$ . Khi đó theo khái niệm về giấu tin an toàn của Cachin [15] ta có định nghĩa sau:

*Định nghĩa 1.1 – Một lược đồ (thuật toán) giấu tin được gọi là an toàn nếu sai phân Kullback – Leibler giữa hàm mật độ xác suất của  $P_C$  và  $P_S$  theo (1.1) là bằng 0*

$$D_{KL}(P_C // P_S) = \sum_{C \in \mathcal{C}} P_C(C) \log \frac{P_C(C)}{P_S(C)} \quad (1.1)$$

*Khi  $D_{KL}(P_C // P_S) < \varepsilon$  thì lược đồ giấu tin có độ an toàn  $\varepsilon$  ( $\varepsilon$  - secure), trong đó  $\varepsilon$  là một số thực dương đủ nhỏ tùy ý cho trước.*

Đây là khái niệm đứng từ quan điểm lý thuyết, nó rất khó thực hiện trong thực tế vì một lược đồ giấu tin để đảm bảo  $D_{KL}(P_C // P_S) = 0$  là không thể vì điều này nghĩa là không thay đổi gì trên ảnh gốc, tức là  $P_C = P_S$  (theo bổ đề cơ bản trong Lý thuyết thông tin). Vì vậy, người ta thường giấu sao cho đạt độ an toàn  $\varepsilon$  - secure đảm bảo thay đổi trên ảnh nhỏ nhất mà mắt người không thể cảm nhận.

Tuy nhiên, rất nhiều lược đồ giấu tin [25, 45, 49, 52, 62, 90, 91, 93, 99] chủ yếu sử dụng đánh giá khả năng cảm nhận của con người dựa vào độ đo PSNR (Peak signal to noise ratio) giữa ảnh gốc ban đầu và ảnh sau khi giấu tin [89]. PSNR là phương pháp đánh giá độ an toàn dựa theo hướng tiếp cận chủ quan. Theo hướng tiếp cận này thì cảm nhận của con người được phân làm năm mức khác nhau. Trên mỗi mức, chất lượng ảnh sẽ được tính theo PSNR, sau đó tùy vào giá trị tính được mà ảnh sẽ được đánh giá là thuộc vào ngưỡng nào. Chất lượng PSNR được ánh xạ vào thang đo đánh giá bình quân MOS (Mean Opinion Score) theo bảng 1.1.

**Bảng 1.1.** Mối quan hệ giữa các giá trị PSNR và MOS

| PSNR [dB] | MOS            |
|-----------|----------------|
| > 37      | 5 (Rất tốt)    |
| 31 - 37   | 4 (Tốt)        |
| 25 – 31   | 3 (Trung bình) |
| 20 – 25   | 2 (Tồi)        |
| < 20      | 1 (Rất tồi)    |

Nhiều kỹ thuật giấu tin như [25, 45, 49, 52, 62, 90, 91, 93, 99] thường cố gắng tác động lên ảnh sau khi giấu tin làm cho chất lượng ảnh theo đánh giá PSNR nằm ở mức 5, với giá trị của PSNR từ 39 dB – 46 dB.

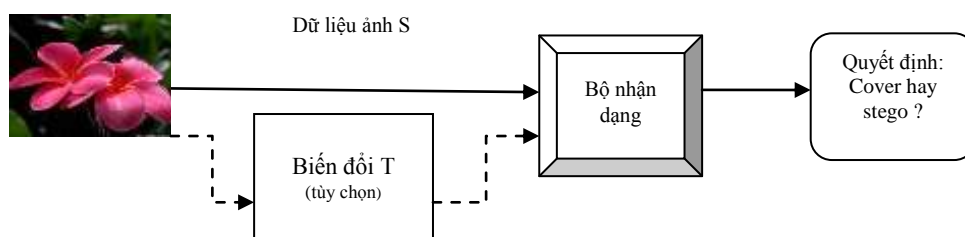
## 1.2. PHÁT HIỆN ẢNH GIẤU TIN VÀ CÁC NGHIÊN CỨU LIÊN QUAN

### 1.2.1. Khái niệm

Phát hiện ảnh giấu tin (image steganalysis) là kỹ thuật phát hiện sự tồn tại của thông tin mật được giấu trong ảnh số [27].

Giống như thám mã, mục đích của *steganalysis* là phát hiện ra đối tượng ảnh số mang thông tin ẩn và phá vỡ tính bí mật của vật mang tin đó.

Hình 1.4 mô tả quá trình tổng quát của kỹ thuật phát hiện ảnh giấu tin. Trong đó phép biến đổi T là phép biến đổi rời rạc cosine, wavelet, hoặc biến đổi sai phân ... (trong một số trường hợp cần thiết).



Hình 1.4. Sơ đồ quá trình phát hiện ảnh có giấu tin [84]

### 1.2.2. Phương pháp phát hiện ảnh có giấu tin

*Phát hiện ảnh giấu tin* có thể định nghĩa như một bài toán phân loại dựa trên kiểm định giả thuyết thống kê. Điều này phụ thuộc vào sự hiểu biết của chúng ta về lược đồ giấu tin, do đó *phát hiện ảnh giấu tin* được phát biểu: hoặc như bài toán kiểm định giả thuyết đơn (simple hypothesis); hoặc như bài toán kiểm định giả thuyết phức hợp (composite hypothesis).

Nếu chúng ta không có thông tin gì về lược đồ giấu tin thì phương pháp phát hiện gọi là phát hiện mù (blind steganalysis), bài toán phân loại có thể phát biểu dựa trên kiểm định giả thuyết phức hợp:

$H_0$ : X được rút ra từ hàm phân bố xác suất là  $P_S$

$H_1$ : X không được rút ra từ hàm phân bố xác suất  $P_S$

Với X là mẫu dữ liệu ảnh được xét.

Trong trường hợp biết trước thông tin về lược đồ giấu tin thì phương pháp phát hiện gọi là phát hiện có ràng buộc (constraint steganalysis). Giả sử chúng ta biết được phân bố xác suất của  $P_C$ , lược đồ giấu tin ( $S_E, S_X$ ) và phân bố của thông tin M, chúng ta có thể tính được  $P_S$ . Từ đó chúng ta có thể đưa ra phương pháp phát hiện có ràng buộc như bài toán phân loại dựa trên kiểm định giả thuyết đơn:

$H_0$ : X có phân bố xác suất là  $P_S$

$H_1$ : X có phân bố xác suất là  $P_C$

Để giải quyết bài toán kiểm định giả thuyết thống kê này, chúng ta cần tìm ra được miền điều kiện của ảnh gốc và ảnh có giấu tin.

Giả sử, bộ phát hiện được miêu tả như một ánh xạ  $F: \Omega \rightarrow \{0, 1\}$ , với  $F(X)=0$ , X được phát hiện là ảnh gốc, với  $F(X) = 1$ , X được cho là ảnh có giấu tin. Khi đó ta có tập miền ràng buộc  $\Omega_1 = \{X \in \Omega \mid F(X) = 1\}$ .

Vậy việc giải quyết bài toán kiểm định giả thuyết thống kê trên tương đương với việc chia tập  $\Omega$  thành hai phần rời nhau:  $\omega$  và  $\Omega \setminus \omega$ . Rõ ràng là có nhiều cách chia khác nhau, dù chia cách nào cũng sẽ xảy ra hai sai lầm: sai lầm loại I, là sai số xảy ra khi thực tế là  $X \in \omega$  nhưng ta lại gán cho  $X \in \Omega \setminus \omega$ , với xác suất  $\alpha$  ( $0 < \alpha < 1$ ) và sai lầm loại II là sai lầm xảy ra khi thực tế là  $X \in \Omega \setminus \omega$  nhưng ta lại gán cho  $X \in \omega$  với xác suất  $\beta$  ( $0 < \beta < 1$ ).

Xác suất  $\alpha$  và  $\beta$  với bộ phát hiện F có thể biểu diễn toán học như sau:

$$\alpha = P(F(X)=1 \mid X \sim P_C) = \int_{\omega} P_C(X) dx$$

$$\beta = P(F(X)=0 \mid X \sim P_S) = \int_{\Omega \setminus \omega} P_S(X) dx$$

Một bộ phát hiện là chấp nhận được nếu thỏa mãn (1.2)

$$(1 - \alpha) \log \left( \frac{1-\alpha}{\beta} \right) + \alpha \log \left( \frac{\alpha}{1-\beta} \right) \leq D_{\text{KL}}(\mathbf{P}_C \parallel \mathbf{P}_S) \quad (1.2)$$

Không có thuật toán chia nào làm cực tiểu hóa cả hai sai lầm này đồng thời. Trong thực tế, người ta thường cố định xác suất sai lầm loại I (cho trước xác suất  $\alpha$ ) và tìm thuật toán phân loại sao cho sai lầm loại II (xác suất  $\beta$ ) là nhỏ nhất. Bài toán phân hoạch không gian làm hai miền  $\omega$  và  $\Omega \setminus \omega$  tương đương bài toán xác định ngưỡng  $T$  (threshold) sao cho nếu một phần tử  $x$  nào đó có đặc trưng thống kê vượt quá ngưỡng  $T$  thì ta bác bỏ giả thuyết  $H_0$ , ngược lại chấp nhận giả thuyết  $H_0$ .

Theo hướng phát hiện dựa trên lý thuyết thống kê bậc lộ sự khác biệt cơ bản giữa phát hiện có ràng buộc và phát hiện mù, phát hiện có ràng buộc chúng ta có thể đưa ra bài toán phát hiện tối ưu dựa trên những hiểu biết về lược đồ giấu tin biết trước, còn phát hiện mù dựa trên kiểm định phức hợp thì bài toán tối ưu của nó thuộc lớp bài toán tấn công mù và kết quả của chúng phụ thuộc chủ yếu vào tỷ lệ thông tin đem nhúng, tỷ lệ nhúng càng cao thì độ chính xác càng lớn.

### 1.2.3. Nghiên cứu liên quan và hướng phát triển của luận án

Các phương pháp nghiên cứu ảnh có giấu tin tập trung vào hai hướng chính như đã nêu trên:

- Hướng thứ nhất cố gắng xây dựng phát hiện mù cho kỹ thuật giấu bất kỳ.
- Hướng thứ hai tìm cách phát hiện ảnh stego khi biết kỹ thuật giấu tin (phát hiện có ràng buộc).

Trong luận án này chỉ đi sâu vào nghiên cứu kỹ thuật phát hiện mù cho ảnh có giấu tin trên LSB và kỹ thuật phát hiện có ràng buộc cho kỹ thuật giấu HKC, DIH, IWH, RVH. Còn các kỹ thuật phát hiện mù khác cho các kỹ thuật giấu SS, QIM, kỹ thuật giấu tin trên ảnh JPEG có thể tham khảo luận án tiến sỹ của K. Sullivan [84] và của Tomás Pevný [66].

Sau đây giới thiệu sơ lược một số kỹ thuật phát hiện mù cho ảnh có giấu tin trên LSB tiêu biểu, phát hiện có ràng buộc cho một số kỹ thuật giấu đã biết và từ đó đưa ra hướng phát triển các kỹ thuật phát hiện trong luận án.

### 1.2.3.1. Phương pháp phát hiện mù cho ảnh giấu trên LSB

#### 1. Một số phương pháp phát hiện mù tiêu biểu

Phương pháp phát hiện mù trên LSB được công bố sớm nhất là kỹ thuật  $\chi^2$  (chi-squared) của A. Westfeld và cộng sự (năm 1999) [95], có khả năng phân biệt một ảnh bất kỳ có hay không giấu tin sử dụng kỹ thuật giấu LSB mà không cần ảnh gốc. Giả sử dữ liệu ảnh được biểu diễn bằng vector  $\{x_i\}_{i=0}^{255}$  với  $x_i$  là tần suất của điểm ảnh  $i$ . Gọi  $(x_{2j}, x_{2j+1})$  với  $0 \leq j \leq 127$ , là các cặp giá trị PoV (Pair of Value). Dựa trên quan sát giữa tập ảnh gốc và tập ảnh có giấu tin (bằng các kỹ thuật giấu LSB) thấy rằng: với tập ảnh giấu tin giá trị của các cặp PoV là xấp xỉ bằng nhau, trong khi với tập ảnh gốc thì giá trị của các cặp PoV là chênh lệch nhau. Điều này có thể giải thích theo ví dụ minh họa trong hình 1.3 cho cặp điểm ảnh có giá trị (116, 117), một điểm ảnh có giá trị là 116 sau khi giấu một bit “1” nó chuyển thành 117, còn giấu một bit “0” nó vẫn giữ nguyên 116, còn điểm ảnh có giá trị là 117, sau khi giấu một bit “1” nó vẫn giữ nguyên giá trị, còn giấu một bit “0” nó chuyển thành 116. Vì vậy khi lượng thông tin giấu càng lớn làm cho giá trị của các cặp PoV càng cân bằng hơn với giả thiết chuỗi bit thông tin có phân bố ngẫu nhiên i.i.d (Independent and Identically Distributed) [95, 29] nên xác suất số bit “0” bằng số bit “1” ( $P(0) \approx P(1)=0.5$ ). Từ vấn đề quan sát đó họ đưa ra phương pháp phát hiện bằng thống kê  $\chi^2$  với  $n-1$  bậc tự do trên các cặp PoV của ảnh. Giá trị  $n$  được xác định từ số các cặp PoV có giá trị lớn hơn 0.

Đến năm 2001, N. Provos đã áp dụng phương pháp thống kê trên của A. Westfeld cho phát hiện ảnh có giấu tin trên LSB của các hệ số cosine [71].

Trong luận án tiến sỹ của K. Sullivan [84] (2005) đưa ra phương pháp phát hiện mù khác cho ảnh giấu trên LSB dựa trên tiêu chuẩn tỉ lệ hợp lý logarit LLRT (Logarit likelihood ratio test). Tác giả sử dụng kiểm định giả thuyết thống kê phức hợp giữa hai giả thuyết  $H_0$  và  $H_R$  (ảnh có giấu tin với tỉ lệ giấu  $0 < R \leq 1$ ), sau đó họ tìm cách quy về hai giả thuyết  $H_0$  (ảnh không giấu tin) và đối thuyết  $H_{R_0}$  (ảnh có giấu tin với tỉ lệ giấu  $R_0$ ). Để tìm ngưỡng phân loại cho ảnh thuộc một trong hai giả

thuyết này K. Sullivan sử dụng phương pháp tối ưu cho bài toán phân loại bằng cách áp dụng tiêu chuẩn tỉ lệ hợp lý logarit LLRT theo sai phân Kullback – Leibler giữa  $p$  (là tập các mật độ xác suất của các tần suất trong ảnh gốc) và  $q$  (là tập các mật độ xác suất tương ứng trong ảnh quan sát) theo định nghĩa sau:  $D(p||q) = \sum_{k=0}^{255} p_k \log \frac{p_k}{q_k}$ , khi đó tiêu chuẩn LLRT sẽ đưa dữ liệu mẫu cần kiểm tra có ẩn thông tin nếu:  $D(q||Q_{R_0p}) - D(q||p) \leq T(\alpha)$ , với  $Q_{R_0p}$  là hàm thay đổi các phần tử của  $p$  với một lượng thông tin có tỉ lệ  $R_0$ . Phương pháp này đòi hỏi phải biết trước ảnh gốc để kiểm tra, tuy nhiên trong thực tế điều này là khó khăn do đó Sullivan đưa ra phương pháp ước lượng mẫu dữ liệu của ảnh gốc từ ảnh cần kiểm tra (ước lượng  $p$  từ  $q$ ) bằng cách sử dụng phương pháp lọc theo đáp ứng xung chiều dài hữu hạn FIR 2-tap (0.5,0.5) (chiều dài bộ lọc bằng hai với hai đáp ứng xung  $h(1)=0.5$ ,  $h(2) = 0.5$ )[11].

Một hướng nghiên cứu khác cho phát hiện mù ảnh có giấu tin trên LSB đó là tìm cách ước lượng tỉ lệ bit thông tin giấu trên LSB. Kỹ thuật ước lượng tiên phong theo hướng này là kỹ thuật RS (Regular and Singular) của Jessica Fridrich và các cộng sự (2001) [31]. Kỹ thuật RS ước lượng bằng cách phân miền dữ liệu ảnh ra thành các miền con nhỏ hơn cùng kích cỡ, thống kê số miền con đều đặn  $R$  (Regular) và dị thường  $S$  (Singular) bằng một mặt nạ phụ trợ  $M$  với hai hàm Hamming  $F_1$  và  $F_{-1}$ , trên ảnh tự nhiên tần suất của miền  $R$  và  $S$  là khác nhau, trong khi với ảnh có giấu tin các giá trị này tiến gần nhau nếu tỉ lệ bit giấu là 50% miền LSB của ảnh. Từ đó họ xây dựng phương trình bậc hai hồi quy dựa trên các miền  $R$  và  $S$  thống kê được để có thể ước lượng xấp xỉ tỉ lệ bit giấu trên LSB.

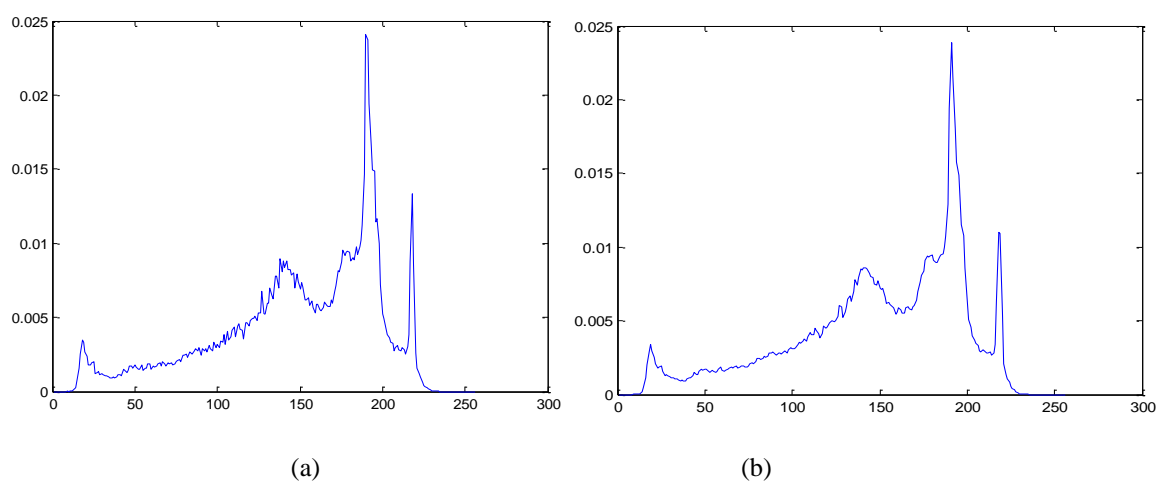
Để cải thiện khả năng ước lượng tỉ lệ bit giấu trên LSB của kỹ thuật RS, năm 2003, T. Zhang và cộng sự đưa ra một phương pháp ước lượng khác dựa trên phân tích các hệ số sai phân (gọi là kỹ thuật DI) [102]. Từ biểu đồ tần suất các hệ số sai phân này có thể thấy được sự tương quan giữa các điểm ảnh liên tiếp trong ảnh, tác giả thấy một sự khác biệt rõ rệt mối tương quan của các hệ số sai phân giữa ảnh gốc và ảnh có giấu tin. Từ đó họ xây dựng phương trình bậc hai để ước lượng tỉ lệ bit thay đổi giữa các điểm ảnh dựa trên biểu đồ hệ số sai phân, sự thay đổi này chính là

tỉ lệ bit thông tin đã giấu trên miền LSB của ảnh. Dựa trên thử nghiệm so sánh giữa kỹ thuật DI và kỹ thuật RS, họ chỉ ra rằng phương pháp của họ ước lượng tốt hơn.

## 2. Hướng phát triển phương pháp phát hiện mù của luận án

Với kỹ thuật phát hiện bằng thống kê  $\chi^2$  với n bậc tự do tỏ ra hiệu quả khi tỉ lệ thông tin giấu lớn hoặc bằng khả năng lớn nhất cho phép của ảnh và được giấu bằng phương pháp tuần tự vào các điểm ảnh. Tuy nhiên, hiệu quả của phương pháp này không cao khi lượng bit thông tin giấu nhỏ và được giấu vào các điểm ảnh theo chiều quét raster (từ trái sang phải, từ trên xuống dưới) trên ma trận dữ liệu ảnh, do đó luận án đưa ra phương pháp khác để cải thiện cho trường hợp này bằng phân tích độ lệch chuẩn và thống kê  $\chi^2$  một bậc tự do.

Với kỹ thuật phát hiện bằng LLRT của K. Sullivan có thể phát hiện tốt cho ảnh đã giấu tin trên LSB nhưng không tốt cho phân loại ảnh gốc. Vì tác giả đưa ra phương pháp ước lượng xấp xỉ dữ liệu ảnh gốc bằng lọc đáp ứng xung FIR từ dữ liệu ảnh cần kiểm tra, lọc bằng FIR thường cho dữ liệu lọc tín hiệu “trơn” (Smoothness) hơn ảnh gốc. Theo ví dụ sau, giả sử một ảnh gốc Baboon.bmp (kích cỡ  $512 \times 512$  điểm ảnh), ta có tập p các mật độ xác suất theo tần suất (histogram) của ảnh Lena.bmp (hình 1.4 a), sử dụng lọc thông thấp FIR cho chính ảnh gốc này từ p ta được tín hiệu lọc q (hình 1.5 b). Rõ ràng tín hiệu sau khi lọc bằng FIR “trơn” hơn tín hiệu gốc, khi đó sử dụng phát hiện bằng LLRT sẽ kết luận ảnh Baboon.bmp là ảnh có giấu tin.



Hình 1.5. biểu đồ mật độ xác suất: a) của tập p, b) của tập p sau khi lọc bằng FIR



Từ phân tích trên với các ảnh nhiễu LLRT sẽ cho kết quả phân loại ảnh gốc chính xác không cao. Do đó trong luận án phương pháp khác dựa trên phân tích tỉ lệ xám bằng bổ đề Neyman – Pearson, đây là bổ đề được cho là tối ưu với các bài toán kiểm định giả thuyết thống kê [108, 109, 110] với trường hợp xác suất  $\alpha$  của sai lầm loại I cho trước, cực tiểu hóa xác suất  $\beta$  của sai lầm loại II. Phương pháp này cũng có thể áp dụng cho ảnh có giấu tin trên hệ số của miền tần số. Chi tiết phương pháp được trình bày trong chương 2.

Với phương pháp phát hiện mù bằng cách ước lượng tỉ lệ bit giấu trên LSB của miền không gian luận án đưa ra phương pháp khác dựa trên lý thuyết trùng khớp, cho kết quả ước lượng tương đương với kỹ thuật ước lượng RS [31] của J. Fridrich và kỹ thuật DI [102] của T. Zhang, nhưng thời gian thực hiện nhanh hơn trên cùng một tập ảnh thử nghiệm. Chi tiết của phương pháp được trình bày trong chương 2.

### ***1.2.3.2. Phương pháp phát hiện ảnh có ràng buộc***

#### **1. Một số phương pháp phát hiện có ràng buộc tiêu biểu**

Trong nhiều trường hợp kỹ thuật giấu biết trước là trường hợp riêng của kỹ thuật giấu LSB với lượng thông tin giấu thấp, làm cho sự thay đổi trong ảnh không lớn lắm, dẫn đến các kỹ thuật phát hiện mù cho ảnh sử dụng các kỹ thuật giấu biết trước này cho độ tin cậy không cao. Do đó, nhà phân tích thường tìm cách đưa ra phương pháp phát hiện tối ưu hơn dựa trên đặc trưng của ảnh trước và sau khi giấu, tìm ra các đặc trưng đặc biệt để có thể phân loại tốt ảnh stego theo các kỹ thuật giấu này. Sau đây là một số phương pháp phát hiện có ràng buộc tiêu biểu.

Kỹ thuật phát hiện cho ảnh giấu tin sử dụng kỹ thuật giấu F5 của Jessica Fridrich và cộng sự (2006) [33] trên hệ số cosine dựa trên phương pháp xây dựng xấp xỉ ảnh gốc từ ảnh quan sát bằng cách cắt đi bốn hàng điểm ảnh trên cùng và bốn hàng điểm ảnh bên trái của dữ liệu ảnh, theo tác giả khi đó hệ số cosine của ảnh sau khi cắt sẽ xấp xỉ ảnh gốc ban đầu, từ đó có thể phát hiện ảnh dựa vào tỉ lệ thay đổi của các hệ số cosine giữa ảnh kiểm tra và ảnh gốc xây dựng được.

Tân công kỹ thuật giấu RCM của Yeh - Shun Chen và cộng sự (2008) [24] bằng cách xác định sự thay đổi của xác suất bit “0”  $P(0)$  và bit “1”  $P(1)$  trên miền LSB, với ảnh gốc thì  $P(0) \approx P(1) \approx 0.5$ , còn với ảnh có giấu tin thì  $P(0) \neq P(1)$ .

Tân công kỹ thuật giấu MBNS của Li Bin và cộng sự (2008) [14], bằng phân tích ngược trên ảnh có giấu tin sử dụng MBNS, họ chứng minh được rằng một lượng thay đổi nhỏ giá trị dư của các điểm ảnh với các hệ số trong MBNS, trong khi điều này không xảy ra với ảnh gốc, từ đó đưa ra được phương pháp phát hiện và ước lượng tỉ lệ giấu dựa vào số lượng các giá trị dư tìm thấy.

Tân công kỹ thuật giấu HKC của Wen – Chung Kuo và cộng sự (2008) [46] được thực hiện bằng cách phân tích biểu đồ tần suất của ảnh gốc và ảnh có giấu tin sử dụng HKC, tác giả phát hiện các ảnh có giấu tin có dấu hiệu không bình thường xung quanh cột tần suất có giá trị lớn nhất. Từ đó đưa ra định lý và thuật toán phát hiện tương ứng.

## **2. Hướng phát triển các phương pháp phát hiện có ràng buộc của luận án**

Bằng việc đi sâu vào tìm hiểu và nghiên cứu một số phương pháp phát hiện có ràng buộc của các tác giả khác chúng ta có thể hiểu được phương pháp họ đã áp dụng từ đó có thể vận dụng, phát triển và mở rộng cho việc phát hiện các kỹ thuật giấu khác, cụ thể trong luận án này đã cải tiến và đưa ra một số kỹ thuật phát hiện có ràng buộc khác cho ảnh có giấu tin sau:

Với phương pháp phát hiện của Wen – Chung Kuo cho kỹ thuật giấu HKC, tác giả đã đưa ra phương pháp phát hiện dựa trên điểm ảnh có tần suất lớn nhất, tuy nhiên chỉ tốt trong trường hợp thông tin được giấu với tỉ lệ giấu lớn nhất có thể của ảnh (thông tin được giấu hết vào các điểm ảnh lân cận điểm ảnh có tần suất lớn nhất), còn các trường hợp khác thì biểu thức mà họ đưa ra dùng để phát hiện không phù hợp. Từ đó luận án đưa ra phương pháp hiệu chỉnh của Wen – Chung Kuo có thể phát hiện hiệu quả hơn và xây dựng một biểu thức phát hiện khác có thể phát hiện trong trường hợp ảnh giấu với tỉ lệ thấp nhất và nhiều nhất sử dụng kỹ thuật

giấu HKC. Ngoài ra luận án còn đưa ra phương pháp ước lượng xấp xỉ bit thông tin giấu trong ảnh mà kỹ thuật phát hiện của Wen – Chung Kuo chưa đưa ra.

Cũng dựa trên phương pháp phân tích biểu đồ tần suất luận án đưa ra phương pháp phát hiện ảnh có giấu tin trên miền hệ số sai phân của kỹ thuật giấu DIH và miền hệ số wavelet của kỹ thuật giấu IWH.

Còn với kỹ thuật giấu RVH hai pha ngang dọc, ta có thể phát hiện dựa trên mở rộng kỹ thuật phát hiện RCM của Chen và các cộng sự như sau: Nếu tính xác suất bit “0” và bit “1” trên LSB của miền điểm ảnh của ảnh có giấu tin thì nó xấp xỉ bằng nhau giống như các ảnh tự nhiên, nhưng khi khảo sát biểu đồ tần suất các điểm ảnh trên các cột lẻ của ảnh hoặc hàng chẵn của ảnh, chúng ta thấy tần suất của các điểm ảnh chẵn lớn hơn các điểm ảnh lẻ (nghĩa là  $P(0) > P(1)$ ) hoặc ngược lại ( $P(1) > P(0)$ ). Vì vậy chúng ta có thể đưa ra được phương pháp phát hiện phù hợp dựa trên  $P(0)$  và  $P(1)$  cho thống kê trên các cột lẻ, hoặc trên các hàng chẵn của ma trận dữ liệu ảnh. Chi tiết các phương pháp phát hiện có ràng buộc sẽ được trình bày chi tiết trong chương 3.

### **1.3. PHƯƠNG PHÁP THỰC NGHIỆM VÀ ĐÁNH GIÁ**

#### **1.3.1. Tiêu chuẩn đánh giá**

Phát hiện ảnh có giấu tin thực chất là bài toán phân lớp tập ảnh bất kỳ vào tập ảnh gốc và tập ảnh có giấu tin. Với phương pháp phân lớp này, nhà phân tích thường sử dụng các độ đo đánh giá: độ chính xác  $P$  (*precision*), độ bao phủ  $R$  (*recall*) và độ trung bình điều hòa  $F$  (*f-measure*) áp dụng cho kỹ thuật phát hiện đề xuất để có thể đánh giá khách quan hiệu quả và độ tin cậy của kỹ thuật.

Giả sử ta có một tập ảnh đầu vào  $\mathcal{E}$  (gồm cả ảnh giấu tin và ảnh chưa giấu tin) cần phân thành 2 tập con  $\mathcal{E}_1$  (ảnh có giấu tin) và  $\mathcal{E}_2$  (ảnh không giấu tin). Sau khi thực hiện phân lớp chúng ta có kết quả phân lớp theo bảng 1.1.

**Bảng 1.1. Bảng phân lớp đối tượng trong tập  $\mathcal{E}$**

|                           |                 | Ảnh có giấu tin | Ảnh không giấu tin |
|---------------------------|-----------------|-----------------|--------------------|
| Kết quả phân lớp đạt được | $\mathcal{E}_1$ | tp              | fp                 |
|                           | $\mathcal{E}_2$ | fn              | tn                 |

Trong đó tp, tn là số khẳng định đúng và phủ định đúng, còn fp, fn là số khẳng định sai và phủ định sai (chính là sai số loại I và sai số loại II). Sau đây là các định nghĩa liên quan đến các độ đo theo [44, 63].

*Định nghĩa 1.2 – Độ chính xác P của tác vụ phân loại ảnh giấu tin là tỉ lệ giữa số ảnh khẳng định đúng so với tổng số ảnh khẳng định đúng và khẳng định sai, được tính theo công thức sau:*

$$P = \frac{tp}{tp+fp} \quad (1.3)$$

*Định nghĩa 1.3 – Độ bao phủ R của tác vụ phân loại ảnh giấu tin là tỉ lệ giữa số ảnh khẳng định đúng so với tổng số ảnh khẳng định đúng và phủ định sai, được tính theo công thức sau:*

$$R = \frac{tp}{tp+fn} \quad (1.4)$$

Mặc dù P và R là những độ đo được dùng rộng rãi và phổ biến nhất, nhưng chúng lại gây khó khăn khi phải đánh giá các hệ thống vì hai độ đo trên lại không tăng/giảm tương ứng với nhau. Hệ thống có R cao có thể có P thấp và ngược lại. Hơn nữa, việc so sánh mà chỉ dựa trên một mình P và R không phải là một ý hay. Với mục tiêu này, độ đo *F-measure* được sử dụng để đánh giá chung cho các hệ thống.

*Định nghĩa 1.4 – Độ trung bình điều hòa F là độ đo trung bình điều hoà có trọng số của P và R theo công thức:*

$$F_{\beta} = (1+\beta^2) \cdot \frac{P \cdot R}{\beta^2 \cdot P + R} \quad (1.5)$$

trong đó  $\beta$  là một tham số có giá trị nằm giữa 0 và 1.

Nếu  $\beta = 1$ , ta có

$$F_1 = 2 \cdot \frac{P \cdot R}{P+R} \quad (1.6)$$

Từ đây ký hiệu F được dùng cho trường hợp  $F_1$  với  $\beta=1$ .

Sử dụng các độ đo P, R, F để đánh giá khả năng phân loại ảnh của các kỹ thuật phát hiện trong luận án hoặc so sánh hiệu quả của kỹ thuật phát hiện đề xuất với các kỹ thuật phát hiện khác. Nếu P càng cao thể hiện độ chính xác và tính đúng đắn trong việc phát hiện ảnh có giấu tin, còn R càng cao thể hiện khả năng phân loại tốt cho ảnh không giấu tin. Vậy một thuật toán có giá trị P, R, F cao thể hiện kỹ thuật phát hiện có khả năng phân loại tốt cho cả tập ảnh giấu tin và tập ảnh không giấu tin (ảnh gốc).

Trong luận án có nhiều phương pháp ước lượng thông tin giấu trong ảnh, để đánh giá độ tin cậy của thuật toán ước lượng được trên một tập ảnh luận án sử dụng giá trị trung bình và độ lệch chuẩn để tính theo khái niệm sau trong [64, 108]:

*Định nghĩa 1.5 - Độ lệch chuẩn (Standard deviation): Cho một tập hữu hạn đại lượng ngẫu nhiên  $X=\{x_1, x_2, \dots, x_n\}$ , khi đó độ lệch chuẩn của các đại lượng này được tính như sau:*

$$s = \sqrt{\frac{1}{n} \sum_{i=1}^n (x_i - \bar{x})^2} \quad (1.7)$$

Với  $n$  là số các thành phần ngẫu nhiên, và  $\bar{x}$  là giá trị trung bình của các đại lượng ngẫu nhiên tính theo công thức (1.8)

$$\bar{x} = \frac{1}{n} (x_1 + x_2 + \dots + x_n) = \frac{1}{n} \sum_{i=1}^n x_i \quad (1.8)$$

### 1.3.2. Nguồn dữ liệu ảnh thử nghiệm

Một vấn đề quan trọng trong luận án chính là việc chuẩn bị các tập dữ liệu ảnh nhằm thực hiện các thực nghiệm liên quan. Nguồn dữ liệu được chọn phải đảm bảo các yêu cầu sau:

- Có độ tin cậy nhất định

- Được công bố bởi các tổ chức có uy tín
- Có số lượng ảnh tương đối lớn
- Nội dung ảnh đa dạng

Hiện nay trên Internet có nhiều thư viện ảnh trực tuyến có độ tin cậy, trong luận án này sử dụng một số ảnh trong hai thư viện trực tuyến [103, 107] của hai trường đại học nổi tiếng Washington, Southern California. Đây là các thư viện được tham khảo và sử dụng trong rất nhiều công trình xử lý ảnh, giấu tin và phát hiện ảnh có giấu tin.

Một phần ảnh được tạo ra từ máy ảnh kỹ thuật số Sony T700 với số điểm ảnh hiệu dụng 10.1 Megapixel, độ phân giải ảnh lớn nhất:  $3648 \times 2736$  điểm ảnh và điện thoại di động Samsung Galaxy 3 với số điểm ảnh hiệu dụng 3.15 Megapixel, độ phân giải ảnh lớn nhất  $2048 \times 1536$  điểm ảnh.

*Tập ảnh gốc thử nghiệm:* Tập ảnh gốc sử dụng chung cho các thuật toán giấu và phát hiện trong luận án gồm 2088 ảnh với các kích cỡ khác nhau trong đó: 1014 ảnh được tải về từ hai thư viện trực tuyến [103, 107] và 1074 ảnh được tạo ra từ máy ảnh kỹ thuật số và máy ảnh trên điện thoại di động. Nội dung ảnh đa dạng gồm: ảnh phong cảnh, chân dung, bản vẽ, vệ tinh, các sự kiện, ...

*Tiền xử lý:* Đa số các ảnh trên là định dạng JPEG ảnh 24 bit màu với ba kênh màu R, G, B. Để thuận tiện cho các tính toán trong thử nghiệm chúng ta chuyển ảnh sang dạng ảnh cấp xám 8-bit cấp độ màu bằng trình xử lý ảnh Adobe Photoshop CS 8.0 được tập ảnh thử nghiệm gồm 2088 ảnh cấp xám. Gọi tập ảnh này là  $\mathcal{C}_0$  sẽ được sử dụng trong hầu hết các thử nghiệm của luận án.

Quá trình thực hiện trên ảnh 24 - bit màu với ba kênh màu R, G, B tương tự như ảnh xám 8-bit bằng cách kiểm tra lần lượt từng kênh 8 - bit R, G, B. Thường thì thông tin giấu trên kênh B, vì theo đánh giá của những nhà giấu tin [27, 32] sẽ ít ảnh hưởng đến chất lượng ảnh.

### **1.3.3. Công cụ hỗ trợ và môi trường thực nghiệm**

Trong thực nghiệm các kỹ thuật đề xuất được cài đặt trên môi trường Matlab phiên bản R2008b (7.7.0), chạy trên máy tính cấu hình Intel (R) Core (TM) 2 Duo T.7200 2.00GHz, bộ nhớ trong 1 Gb, bộ nhớ ngoài có dung lượng tổng khả dụng 15GB. Quá trình thực nghiệm có sự hỗ trợ của phần mềm xử lý ảnh Photoshop phiên bản CS2 8.0 để chuyển đổi dữ liệu ảnh từ màu sang ảnh đa cấp xám thuận tiện tính toán cho các thuật toán.

## **KẾT LUẬN CHƯƠNG 1**

Chương này đưa ra bức tranh tổng quan về giấu tin trong ảnh, phát hiện ảnh có giấu tin và các hướng nghiên cứu liên quan. Với mỗi phương pháp giấu sẽ hình thành nên một số kỹ thuật phát hiện phù hợp thúc đẩy sự phát triển của phương pháp giấu. Việc đi sâu vào tìm hiểu các kỹ thuật phát hiện đó sẽ giúp chúng ta định hướng phát triển và cải tiến kỹ thuật giấu hiện tại hoặc đó chính là nền tảng để mở rộng cho các kỹ thuật phát hiện khác. Ngoài ra, chương này còn giới thiệu một số khái niệm, phương pháp đánh giá, công cụ hỗ trợ và nguồn dữ liệu ảnh dùng để thử nghiệm các kỹ thuật cải tiến đề xuất trong luận án.

Chương tiếp theo sẽ đi vào chi tiết một số kỹ thuật phát hiện mù cho ảnh có giấu tin trên miền LSB.

## **Chương 2. KỸ THUẬT PHÁT HIỆN MÙ CHO ẢNH GIẤU TIN TRÊN LSB**

Chương này đưa ra một số kỹ thuật phát hiện mù cho ảnh có giấu tin trên LSB của miền không gian hoặc miền tần số. Phương pháp phát hiện dựa trên phân tích mẫu dữ liệu ảnh trước và sau khi giấu bằng thay đổi trên LSB để tìm ra đặc trưng khác biệt, từ đó áp dụng một số chuẩn trong thống kê: “độ lệch chuẩn”, “ $\chi^2$  một bậc tự do”, “bài toán kiểm định tối ưu Neyman – Pearson” để xây dựng thuật toán phát hiện phù hợp.

### **2.1. KỸ THUẬT PHÁT HIỆN MÙ TRÊN LSB CỦA MIỀN KHÔNG GIAN**

#### **2.1.1. Phát hiện bằng phân tích “độ lệch chuẩn”**

##### **2.1.1.1. Phân tích kỹ thuật giấu LSB**

Giả sử dữ liệu của một ảnh gốc 8 - bit cấp độ xám được biểu diễn dưới dạng ma trận  $C^{26 \times 10} = \{c_{ij}, i=0, \dots, 25, j=0, \dots, 9\}$  với  $c_{ij}$  là tần suất của điểm ảnh có giá trị bằng  $i \cdot 10 + j$  trong ảnh (ví dụ  $c_{13,2} = 35$ , nghĩa là tần suất của điểm ảnh có giá trị 132 là 35). Sau khi giấu chuỗi thông tin  $M = \{m_i \in \{0,1\}, i=0, \dots, l-1\}$  với  $l = |M|$  được ảnh có giấu tin với ma trận tương ứng  $S^{26 \times 10} = \{s_{ij}, i=0, \dots, 25, j=0, \dots, 9\}$ .

So sánh hai ma trận  $C^{26 \times 10}$  và  $S^{26 \times 10}$ , phát hiện một vấn đề rất quan trọng đó là tổng giá trị trên từng hàng của  $C^{26 \times 10}$  và  $S^{26 \times 10}$  tương ứng là không thay đổi, chỉ có giá trị của các phần tử trong hàng đó là thay đổi. Trong ảnh C trên từng hàng của  $C^{26 \times 10}$  xuất hiện nhiều điểm đột biến, tức giá trị của nó rất khác nhau. Còn với ảnh S thì các giá trị biến thiên rất gần nhau.

Vấn đề khẳng định trên được giải thích như sau: giả sử một cặp điểm ảnh  $(p_1=8, p_2=9)$  (tần suất của nó nằm cuối hàng đầu tiên của  $C^{26 \times 10}$ ), nếu  $p_1$  sau khi giấu một bit “0” thì  $p_1$  vẫn bằng 8 (mặc định được giấu vào  $p_1$ ), nếu giấu một bit “1” thì  $p_1=9$ , còn  $p_2$  sau khi giấu một bit “0” thì  $p_2=8$ , nếu giấu một bit “1” thì  $p_2=9$ . Nghĩa là sau khi giấu tin cặp điểm ảnh  $(p_1, p_2)$  chỉ thay đổi giá trị cho nhau mà không chuyển sang cặp điểm ảnh ở hàng khác. Do đó tổng giá trị trên cùng một hàng của



C là không đổi sau khi giấu tin. Mặt khác khi lượng thông tin giấu càng lớn nó làm cho tần suất của cặp  $(p_1, p_2)$  là xấp xỉ bằng nhau.

Để chứng tỏ vấn đề này bằng cách lấy logarit của tích các  $c_i^{mn}$ ,  $s_i^{mn}$  trên từng dòng tương ứng của  $C^{26 \times 10}$  và  $S^{26 \times 10}$  thấy rằng logarit của ảnh giấu tin lớn hơn ảnh gốc. Còn dòng nào có giá trị logarit xấp xỉ nhau nghĩa là thông tin không giấu hoặc được giấu rất ít trên dòng đó.

Ví dụ cho trước một ảnh gốc và ảnh đã giấu tin có kích cỡ 119x119. Sau khi tính tần suất điểm ảnh của ảnh gốc và ảnh có giấu tin được ma trận  $C^{26 \times 10}$  và  $S^{26 \times 10}$ .

Lấy logarit trên 5 dòng đầu tiên của  $C^{26 \times 10}$  ta được:

$$\begin{aligned} \text{Dòng 1: } \log(29*49*83*84*115*124*162*195*275*239) &= \log(29) + \log(49) \\ &+ \log(83) + \log(84) + \log(115) + \log(124) + \log(162) + \log(195) + \log(275) \\ &+ \log(239) = 20.46735 \end{aligned}$$

$$\begin{aligned} \text{Dòng 2: } \log(238*262*211*199*180*173*119*152*128*103) &= \log(238) + \dots + \\ &\log(103) = 22.28877013 \end{aligned}$$

$$\begin{aligned} \text{Dòng 3: } \log(110*89*95*87*80*55*54*53*58*58) &= \log(110) + \dots + \log(58) = \\ &18.53500384 \end{aligned}$$

$$\begin{aligned} \text{Dòng 4: } \log(50*46*39*46*37*43*43*36*49*44) &= \log(50) + \dots + \log(44) = \\ &16.34064017 \end{aligned}$$

$$\begin{aligned} \text{Dòng 5: } \log(39*34*41*30*25*28*28*40*29*35) &= \log(39) + \dots + \log(35) = \\ &15.11323074 \end{aligned}$$

Lấy logarit trên 5 dòng đầu tiên của  $S^{26 \times 10}$  ta được:

$$\text{Dòng 1: } \log(38*40*86*81*119*120*180*177*260*254) = 20.5026081$$

$$\text{Dòng 2: } \log(246*254*216*194*165*188*145*126*119*112) = 22.29616963$$

$$\text{Dòng 3: } \log(97*102*89*93*72*63*45*62*65*51) = 18.53600564$$

$$\text{Dòng 4: } \log(48*48*41*44*43*37*42*37*45*48) = 16.34629395$$

$$\text{Dòng 5: } \log(36*37*31*40*24*29*36*32*32*32) = 15.13228759$$

Từ các biểu thức logarit trên 5 dòng đầu tiên của  $C^{26 \times 10}$  và  $S^{26 \times 10}$ , ta thấy giá trị logarit trên ảnh có giấu tin ( $S^{26 \times 10}$ ) lớn hơn logarit trên ảnh không có giấu tin ( $C^{26 \times 10}$ ), vì sau khi giấu tin các giá trị tương ứng trên từng cặp giá trị của hàng xấp xỉ bằng nhau làm cho giá trị logarit tăng lên.

Ý tưởng này xuất phát từ việc giải bài toán số học đơn giản sau đây:

Cho trước một đoạn thẳng độ dài  $n$ . Hãy chia đoạn thẳng đó ra  $k$  phần  $a_1, a_2, \dots, a_k$  sao cho tích của chúng lớn nhất, tức là tìm  $a_1, a_2, \dots, a_k$  để tích  $a_1 * a_2 * \dots * a_k$  là lớn nhất.

Cách chia đơn giản nhất là chia sao cho  $a_1 = a_2 = \dots = a_k$

Chính vì vậy ta thấy rằng, khi thông tin giấu vào trong ảnh nó sẽ làm cho các giá trị trong từng hàng của  $S^{26 \times 10}$  san gần bằng nhau, dẫn đến logarit tại hàng đó có giá trị lớn hơn hàng tương ứng trong ảnh gốc. Đây chính là yếu tố quan trọng cho việc phát hiện ảnh có giấu tin sẽ đề cập trong mục tiếp theo.

Lưu ý: Ta có thể lấy tích của từng dòng trong ảnh gốc chia cho tích của từng dòng tương ứng trong ảnh stego, thương thu được có giá trị nhỏ hơn 1. Thương nào có giá trị 1 thì chứng tỏ dòng đó không được nhúng tin. Sở dĩ ta lấy logarit là để giảm tích của chúng quá lớn, nhưng sẽ giảm độ chính xác mỗi lần lấy logarit, thông tin sẽ bị mất. Do đó, chúng ta cần lấy độ chính xác từ 8 đến 10 chữ số thập phân sau dấu “,” giá trị kết quả logarit thu được.

### **2.1.1.2. Phương pháp phát hiện**

Theo phân tích trên luận án đưa ra bài toán phân lớp sau:

**Bài toán:** Cho một tập các ảnh bất kỳ (gồm cả ảnh giấu tin và ảnh chưa giấu tin). Hãy tìm cách phân hoạch tập đó thành 2 tập con  $\mathcal{A}$ ,  $\mathcal{B}$  trong đó  $\mathcal{A}$  là tập gồm các ảnh có giấu tin và tập  $\mathcal{B}$  gồm các ảnh gốc sao cho sai số của việc phân lớp là nhỏ nhất. Hay phát biểu lại theo lý thuyết kiểm định giả thuyết thống kê giữa hai giả thuyết:  $H_0$  giả thuyết ảnh có giấu tin và  $H_1$  đối thuyết ảnh không giấu tin sao cho sai số của bài toán phân lớp là nhỏ nhất.

### *Phương pháp giải*

Giả sử dữ liệu ảnh là các mẫu được lấy từ một họ có phân bố chuẩn  $N(a, \sigma^2)$  với kỳ vọng  $a$  và phương sai  $\sigma^2$  có hàm mật độ xác suất:

$$p(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-a)^2}{2\sigma^2}} \quad \text{với } -\infty < x < \infty$$

Còn phân bố của  $X$  được xác định bằng

$$F(x) = P\{X < x\} = \frac{1}{\sigma\sqrt{2\pi}} \int_{-\infty}^x e^{-\frac{(u-a)^2}{2\sigma^2}} du \quad \text{với } -\infty < x < \infty$$

Tại sao chúng ta lại giả thiết là mẫu được lấy từ họ phân bố chuẩn. Vì ta biết rằng: một ảnh số bất kỳ cũng giống như một văn bản nào đó chẳng hạn là tiếng Anh được viết bằng 26 chữ cái La tinh. Ở đây chỉ khác ở chỗ: ảnh được thể hiện bằng 256 chữ số. Người ta đã chứng minh được rằng, ngôn ngữ tự nhiên được thể hiện như là họ có phân bố tiệm cận chuẩn [109].

*Định Lý 2.1 [108] - Cho  $X$  là đại lượng ngẫu nhiên có phân bố chuẩn  $N(a, \sigma^2)$ . Khi đó đại lượng ngẫu nhiên  $Y = (X - a)/\sigma$  có phân bố chuẩn  $N_n(0, 1)$ .*

*Định lý 2.2 - Cho  $X_1, X_2, \dots, X_n$  là đại lượng ngẫu nhiên, độc lập cùng phân bố chuẩn  $N(a, \sigma^2)$ . Khi đó đại lượng ngẫu nhiên  $X_1 + X_2 + \dots + X_n$  sẽ có phân bố chuẩn  $N(na, n\sigma^2)$ .*

Chứng minh:

Thật vậy, theo tính chất của kỳ vọng toán học ta có kỳ vọng của một tổng bằng tổng các kỳ vọng từng thành phần, do đó kỳ vọng  $E(X_1+X_2+\dots+X_n) = E(X_1) + \dots + E(X_n) = na$ .

Tương tự, do tính độc lập của chúng, ta có phương sai của một tổng bằng tổng các phương sai.

Vậy phương sai  $D(X_1+X_2+\dots+X_n) = D(X_1) + \dots + D(X_n) = n\sigma^2$  (điều phải chứng minh).

Trong thực tế  $a$  và  $\sigma^2$  chưa biết nên ta phải ước lượng  $a, \sigma^2$ . Có nhiều phương pháp để ước lượng các đại lượng này nhưng một phương pháp thông dụng và đơn

giản nhất là phương pháp hợp lý cực đại [109]. Bằng phương pháp này thay a bằng ước lượng  $\bar{x} = \frac{1}{n} \sum_{i=1}^n x_i$  và  $\sigma^2$  bằng ước lượng  $\hat{S}^2 = \frac{1}{n} \sum_{i=1}^n (x_i - \bar{x})^2$ , do đó  $\sigma = \hat{S}$  (đây là ước lượng chệch của  $\sigma^2$  nhưng có phương sai cực tiểu [109]).

Ta ký hiệu:  $x_{\max} = \max\{x_1, x_2, \dots, x_n\}$  và  $x_{\min} = \min\{x_1, x_2, \dots, x_n\}$

Khi đó áp dụng định lý 2.1 ta có các đại lượng ngẫu nhiên:

$$V_1 = \frac{x_{\max} - \bar{x}}{\hat{S}}, \quad V_2 = \frac{\bar{x} - x_{\min}}{\hat{S}}, \text{ sẽ có phân bố chuẩn } N_n(0,1).$$

Do đó  $V = V_1 + V_2$ , theo định lý 2.2, sẽ có phân bố chuẩn  $N_n(0, 2)$ .

Áp dụng định lý giới hạn trung tâm [108, 109], ta có:

$$T = \frac{V}{\sqrt{2}} \tag{2.1}$$

sẽ có phân bố chuẩn  $N_n(0, 1)$  đã được lập thành bảng XII trong [109] với  $n=1, 2, 3, \dots$  và độ tin cậy  $\alpha=0.1, 0.05, \dots$

Đại lượng ngẫu nhiên T từ (2.1) có phân bố chuẩn  $N_n(0, 1)$  tức có xác suất

$$P\{T \geq x_0\} = \int_{x_0}^{\infty} p_n(t) dt$$

trong đó  $p_n(t)$  là hàm mật độ xác suất chuẩn  $N_n(0,1)$ . Nếu cho trước n và giá trị xác suất  $\alpha = \alpha_0$  (sai số loại I), ta có thể tìm được giá trị ngưỡng  $x_0$  từ phương trình:

$$\alpha_0 = \int_{x_0}^{\infty} p_n(t) dt = 1 - \int_{-\infty}^{x_0} p_n(t) dt$$

Đó là những kết quả làm cơ sở để xây dựng thuật toán phát hiện ảnh có giấu thông tin.

Do  $T = \frac{V_1 + V_2}{\sqrt{2}}$  và  $\{T \geq x_0\} \Leftrightarrow \{V_1 + V_2 \geq \sqrt{2} x_0\}$ , nên sau khi xác định được  $x_0$ , ta có thể tìm được ngưỡng theo biểu thức (2.2) sau đây:

$$t_0 = x_0 \sqrt{2} \tag{2.2}$$

Sau khi tìm được ngưỡng chúng ta có thể áp dụng để phân loại ảnh theo thuật toán 2.1.

**Thuật toán 2.1 – Thuật toán “độ lệch chuẩn”**

**Đầu vào:** Cho một ảnh 8-bit cấp độ màu C bất kỳ

**Đầu ra:** Kiểm tra xem ảnh C là ảnh có giấu tin trên LSB hay không.

**Bước 1:** Biểu diễn dữ liệu của ảnh C dưới dạng vector  $Y = \{y_{ij}, i=\overline{0,25}, j=\overline{0,9}\}$ .

**Bước 2:** Tính  $X = \{x_j, x_j = \sum_{i=0}^{25} y_{ij}, j=\overline{0,9}\}$ .

Tìm  $x_{\max} = \max\{x_0, x_2, \dots, x_9\}$ ,  $x_{\min} = \min\{x_0, x_2, \dots, x_9\}$

Ký hiệu  $\bar{x} = \frac{1}{10} \sum_{i=0}^9 x_i$  và  $\hat{S} = \sqrt{\frac{1}{10} \sum_{i=0}^9 (x_i - \bar{x})^2}$

Từ đó ta xác định được  $Z = \frac{x_{\max} - x_{\min}}{\hat{S}}$

**Bước 3:** Kết luận:

- Nếu  $Z \geq t_0$ , kết luận ảnh C không giấu thông tin trên LSB.
- Nếu  $Z < t_0$ , kết luận ảnh C có giấu thông tin trên LSB

Để lựa chọn ngưỡng  $t_0$  phù hợp theo (2.2) với giá trị của  $x_0$  đã được lập theo bảng phân bố chuẩn trong [108], với các giá trị độ tin cậy  $\alpha = 0.1, 0.05, 0.025, 0.01$ , ta được bảng 2.1 giá trị của  $t_0$  theo (2.2).

**Bảng 2.1. Giá trị  $t_0$  ứng với giá trị  $x_0$  theo bảng lập sẵn trong [108]**

| $\alpha$ | <b>0.1</b> | <b>0.05</b> | <b>0.025</b> | <b>0.01</b> |
|----------|------------|-------------|--------------|-------------|
| $x_0$    | 2.146      | 2.294       | 2.414        | 2.540       |
| $t_0$    | 3.035      | 3.244       | 3.414        | 3.592       |

Để lựa chọn  $t_0$  cho kết quả phân loại tốt, luận án thực hiện đánh giá trên cùng tập ảnh  $\mathcal{C}_{0_1}$  gồm 600 ảnh gốc cấp xám lấy từ tập ảnh  $\mathcal{C}_0$  (gồm 2088 gốc ảnh đã giới thiệu trong chương 1), tập ảnh  $\mathcal{C}_{0_1}$  được giấu một lượng thông tin với các tỉ lệ 30%, 50%, 70%, 100% được các tập ảnh có giấu tin tương ứng  $\mathcal{S}_{\text{LSB}_{30}}$ ,  $\mathcal{S}_{\text{LSB}_{50}}$ ,  $\mathcal{S}_{\text{LSB}_{70}}$ ,

$\mathcal{S}_{LSB_{100}}$ . Các tập ảnh này được kiểm tra phân loại dựa vào các giá trị  $t_0$  theo bảng 3.1 ta được kết quả phân loại theo bảng 2.2.

**Bảng 2.2. Phân loại ảnh theo  $t_0$  trên tập  $\mathcal{C}_{0,1}$ ,  $\mathcal{S}_{LSB_{30}}$ ,  $\mathcal{S}_{LSB_{50}}$ ,  $\mathcal{S}_{LSB_{70}}$ ,  $\mathcal{S}_{LSB_{100}}$**

| Tập ảnh \ Ngưỡng $t_0$    | 3.035       |                     | 3.244       |                     | 3.414       |                     | 3.592       |                     |
|---------------------------|-------------|---------------------|-------------|---------------------|-------------|---------------------|-------------|---------------------|
|                           | ảnh gốc (%) | ảnh có giấu tin (%) | ảnh gốc (%) | ảnh có giấu tin (%) | ảnh gốc (%) | ảnh có giấu tin (%) | ảnh gốc (%) | ảnh có giấu tin (%) |
| $\mathcal{C}_{0,1}$       | 90          | 10                  | 56          | 44                  | 36          | 64                  | 13          | 87                  |
| $\mathcal{S}_{LSB_{30}}$  | 57          | 43                  | 41          | 59                  | 24          | 76                  | 8           | 92                  |
| $\mathcal{S}_{LSB_{50}}$  | 48          | 52                  | 36          | 64                  | 21          | 79                  | 7           | 93                  |
| $\mathcal{S}_{LSB_{70}}$  | 35          | 62                  | 32          | 68                  | 19          | 81                  | 6           | 94                  |
| $\mathcal{S}_{LSB_{100}}$ | 8           | 92                  | 6           | 94                  | 3           | 97                  | 1           | 99                  |

Từ bảng 2.2 ta thấy với  $t_0$  có giá trị càng cao thì nó có khả năng phân loại tốt ảnh có giấu tin trên LSB, nhưng không tốt khi phân loại ảnh gốc. Do đó lấy  $t_0 = 3.035$  sẽ cho kết quả phân loại hiệu quả phù hợp với cả ảnh không giấu tin và ảnh có giấu tin.

### 2.1.2. Phát hiện bằng thống kê $\chi^2$ một bậc tự do ( $\chi_1^2$ )

#### 2.1.2.1. Phân tích kỹ thuật “độ lệch chuẩn”

Hạn chế của kỹ thuật “độ lệch chuẩn” là phụ thuộc vào dữ liệu ảnh và độ dài của thông tin đem giấu trong ảnh. Nếu dữ liệu của ảnh có độ nhiễu cao thì khó phát hiện chính xác vì dữ liệu của ảnh phân bố rất đều nên việc phát hiện theo độ “lệch chuẩn” sẽ khó tin cậy. Mặt khác dữ liệu ảnh đem giấu ít cũng khó phát hiện hơn vì nếu dữ liệu đem giấu ít nó gần như không làm thay đổi nhiều dữ liệu ban đầu của ảnh, và do đó ít ảnh hưởng đến sự phân bố đều dữ liệu của ảnh trong biểu thức phát hiện (2.2). Để cho kết quả cải thiện hơn phần này sẽ mở rộng thuật toán “độ lệch chuẩn” bằng cách sử dụng “thống kê  $\chi^2$  một bậc tự do” chi tiết dưới đây.

#### 2.1.2.2. Phương pháp phát hiện

Sử dụng định lý 2.3 trong [108] chúng ta xây dựng bỏ đề 2.1 sau:

*Định lý 2.3 [108]: Gọi  $m$  là số lần xuất hiện một biến cố  $A$  trong dãy  $n$  phép thử Bernouli với xác suất xuất hiện biến cố  $A$  là  $P(A) = p > 0$ .*

*Khi đó, đại lượng ngẫu nhiên  $Y = \frac{m - np}{\sqrt{npq}}$  có xấp xỉ phân bố chuẩn  $N(0, 1)$ , với  $q = 1 - p$ .*

*Bổ đề 2.1. Giả sử cho trước một dãy nhị phân được lấy từ một nguồn ngẫu nhiên, độc lập  $s = s_0, s_1, \dots, s_{n-1}$ . Ký hiệu  $n_0$  và  $n_1$  lần lượt là tần suất số “0” và “1” xuất hiện trong dãy (tức  $n_0 + n_1 = n$ )*

$$\text{Đặt } z = \frac{(n_0 - n_1)^2}{n} \quad (2.3)$$

*Khi đó, nếu  $s$  là ngẫu nhiên, độc lập thì  $z$  có phân bố “ $\chi$  – bình phương” (chi-square) 1 bậc tự do (với  $n \geq 10$ )*

Chứng minh:

Để chứng minh bổ đề, ta chỉ việc chứng minh rằng với dãy  $s$  hoàn toàn ngẫu nhiên, độc lập thì  $\frac{n_0 - n_1}{\sqrt{n}}$  có phân bố chuẩn  $N(0,1)$ .

Thật vậy, ta hãy đặt

$$\chi_k(0) = \begin{cases} 1 & \text{nếu số 0 xuất hiện tại vị trí } k \text{ của dãy } S \\ 0 & \text{nếu ngược lại} \end{cases}$$

$$\text{Rõ ràng rằng } n_0 = \sum_{k=0}^{n-1} \chi_k(0)$$

$$\text{Ta có kỳ vọng của } n_0 \text{ là } E(n_0) = E\left(\sum_{k=0}^{n-1} \chi_k(0)\right) = \sum_{k=0}^{n-1} E(\chi_k(0)) = np$$

Còn phương sai của  $n_0$  là

$$D(n_0) = D\left(\sum_{k=0}^{n-1} \chi_k(0)\right) = \sum_{k=0}^{n-1} D(\chi_k(0)) = \sum_{k=0}^{n-1} [E(\chi_k(0))^2 - (E\chi_k(0))^2] =$$

$$= \sum_{k=0}^{n-1} (p - p^2) = \sum_{k=0}^{n-1} p(1-p) = npq$$

Từ định lý 2.3, ta có:  $\frac{n_0 - np}{\sqrt{npq}}$

là đại lượng ngẫu nhiên có phân bố xấp xỉ chuẩn  $N(0,1)$ .

Trường hợp đặc biệt do  $s$  là dãy ngẫu nhiên, độc lập cùng phân bố nên  $p=q=1/2$ . Ta được:  $\frac{n_0 - np}{\sqrt{npq}} = \frac{2(n_0 - n/2)}{\sqrt{n}} = \frac{2n_0 - n}{\sqrt{n}} = \frac{2n_0 - (n_0 + n_1)}{\sqrt{n}} = \frac{n_0 - n_1}{\sqrt{n}}$

Vậy  $\frac{n_0 - n_1}{\sqrt{n}}$  có phân bố chuẩn  $N(0,1)$

Từ đó  $\left(\frac{n_0 - n_1}{\sqrt{n}}\right)^2 = \frac{(n_0 - n_1)^2}{n}$  có phân bố “ $\chi$  – bình phương” 1 bậc tự do.

Bổ đề được chứng minh.

Áp dụng bổ đề 2.1 vào việc phân loại ảnh có hay không giấu thông tin mật trên LSB, chúng ta xây dựng thuật toán 2.2 sau đây:

### **Thuật toán 2.2 – Thuật toán “ $\chi^2$ một bậc tự do ( $\chi_1^2$ )”**

**Đầu vào:** Cho một ảnh 8-bit cấp độ màu  $C$  bất kỳ

**Đầu ra:** Kiểm tra xem ảnh  $C$  là ảnh có giấu tin trên LSB hay không

**Bước 1:** Tính tần suất điểm ảnh của  $C$  được ma trận  $C^{26 \times 10}$ , bỏ qua hàng cuối cùng của  $C^{26 \times 10}$  vì hàng này có chứa 5 phần tử có giá trị bằng 0, ta được  $C^{25 \times 10}$ .

**Bước 2:** Tìm giá trị lớn nhất của  $C^{25 \times 10}$ .

Ký hiệu là  $x_{\max} = \max\{c_{ij}, i=0, \dots, 24, j=0, 1, \dots, 9\}$

Giả sử giá trị lớn nhất đó là  $x_{\max} = c_{i_0 j_0}$  (giá trị lớn nhất của của  $C^{25 \times 10}$  tại hàng  $i_0$ , cột  $j_0$ .)

**Bước 3:** Tại hàng  $i_0$ , tính tổng chẵn  $n_{i_0}[0] = \sum_{j=0}^4 c_{i_0, 2j}$  và tổng lẻ  $n_{i_0}[1] = \sum_{j=0}^4 c_{i_0, 2j+1}$ ,

Khi đó tổng giá trị của hàng  $i_0$  được  $n_{i_0} = n_{i_0}[0] + n_{i_0}[1]$ .



$$\text{Áp dụng bổ đề 2.1 ta có } z = \frac{(n_{i_0[0]} - n_{i_0[1]})^2}{n_{i_0}}$$

**Bước 4:** Kết luận:

- Nếu  $z \geq \chi_1^2(\alpha)$ , thì C là ảnh không giấu tin trên miền LSB.
- Ngược lại, nếu  $z < \chi_1^2(\alpha)$ , thì C là ảnh có giấu tin trên LSB với xác suất độ tin cậy là  $\alpha$ .

Theo bảng thống kê  $\chi^2$  trong [108, 109] với  $n=1$ , ta có bảng 2.3 theo một số giá trị  $\alpha$ .

**Bảng 2.3. Giá trị  $\chi_1^2$  ứng với giá trị  $\alpha$  theo bảng lập sẵn trong [108]**

|                    |      |      |       |      |       |
|--------------------|------|------|-------|------|-------|
| $\alpha$           | 0.1  | 0.05 | 0.025 | 0.01 | 0.005 |
| $\chi_1^2(\alpha)$ | 2.71 | 3.84 | 5.02  | 6.63 | 7.88  |

Việc lựa chọn giá trị ngưỡng phân loại  $\chi_1^2(\alpha)$  là giá trị nào cho phù hợp trong bảng 2.3, luận án thực hiện thử nghiệm trên năm tập ảnh  $\mathcal{C}_{0,1}$ ,  $\mathcal{S}_{\text{LSB}_{30}}$ ,  $\mathcal{S}_{\text{LSB}_{50}}$ ,  $\mathcal{S}_{\text{LSB}_{70}}$ ,  $\mathcal{S}_{\text{LSB}_{100}}$  (giống như trong 2.1.1). Thực hiện phân loại theo các giá trị  $\chi_1^2(\alpha)$  từ bảng 2.3, được kết quả phân loại theo bảng 2.4.

**Bảng 2.4. Kết quả phân loại ảnh ứng với các giá trị  $\chi_1^2$  trong bảng 2.3**

| Tập ảnh \ $\chi_1^2$             | 2.71        |                     | 3.84        |                     | 5.02        |                     | 6.63        |                     | 7.88        |                     |
|----------------------------------|-------------|---------------------|-------------|---------------------|-------------|---------------------|-------------|---------------------|-------------|---------------------|
|                                  | ảnh gốc (%) | ảnh có giấu tin (%) | ảnh gốc (%) | ảnh có giấu tin (%) | ảnh gốc (%) | ảnh có giấu tin (%) | ảnh gốc (%) | ảnh có giấu tin (%) | ảnh gốc (%) | ảnh có giấu tin (%) |
| $\mathcal{C}_{0,1}$              | 96          | 4                   | 88          | 12                  | 78          | 22                  | 72          | 28                  | 69          | 31                  |
| $\mathcal{S}_{\text{LSB}_{30}}$  | 54          | 46                  | 76          | 24                  | 67          | 33                  | 64          | 36                  | 59          | 41                  |
| $\mathcal{S}_{\text{LSB}_{50}}$  | 41          | 59                  | 60          | 40                  | 61          | 39                  | 59          | 41                  | 57          | 43                  |
| $\mathcal{S}_{\text{LSB}_{70}}$  | 33          | 67                  | 30          | 70                  | 17          | 83                  | 15          | 85                  | 10          | 90                  |
| $\mathcal{S}_{\text{LSB}_{100}}$ | 6           | 94                  | 5           | 95                  | 4           | 96                  | 1           | 99                  | 0           | 100                 |

Dựa vào bảng 2.4, ta thấy  $\chi_1^2(0.1)=2.71$  cho kết quả phân loại phù hợp.

Để đánh giá hiệu quả giữa kỹ thuật  $\chi_1^2$  với kỹ thuật “độ lệch chuẩn”, luận án thực hiện thử nghiệm phân loại trên năm tập  $\mathcal{C}_{0_1}$ ,  $\mathcal{S}_{LSB_{30}}$ ,  $\mathcal{S}_{LSB_{50}}$ ,  $\mathcal{S}_{LSB_{70}}$ ,  $\mathcal{S}_{LSB_{100}}$  bằng phương pháp phát hiện dựa trên  $\chi_1^2$  (với ngưỡng chọn  $\chi_1^2(0.1)=2.71$ ) và kỹ thuật “độ lệch chuẩn”, ta được kết quả theo bảng 2.5.

**Bảng 2.5. Phân loại ảnh trên  $\mathcal{C}_{0_1}$ ,  $\mathcal{S}_{LSB_{30}}$ ,  $\mathcal{S}_{LSB_{50}}$ ,  $\mathcal{S}_{LSB_{70}}$ ,  $\mathcal{S}_{LSB_{100}}$  bằng kỹ thuật “Độ lệch chuẩn” và  $\chi_1^2$**

| Tập ảnh                   | Kỹ thuật “Độ lệch chuẩn” |                     | Kỹ thuật $\chi_1^2$ |                     |
|---------------------------|--------------------------|---------------------|---------------------|---------------------|
|                           | ảnh gốc (%)              | ảnh có giấu tin (%) | ảnh gốc (%)         | ảnh có giấu tin (%) |
| $\mathcal{C}_{0_1}$       | 90                       | 10                  | 96                  | 4                   |
| $\mathcal{S}_{LSB_{30}}$  | 57                       | 43                  | 54                  | 46                  |
| $\mathcal{S}_{LSB_{50}}$  | 48                       | 52                  | 41                  | 59                  |
| $\mathcal{S}_{LSB_{70}}$  | 35                       | 62                  | 33                  | 67                  |
| $\mathcal{S}_{LSB_{100}}$ | 8                        | 92                  | 6                   | 94                  |

Từ bảng 2.5 cho thấy kết quả phân loại bằng kỹ thuật  $\chi_1^2$  cho kết quả tốt hơn kỹ thuật “độ lệch chuẩn”. Mục tiếp theo sẽ đưa ra phương pháp khác phát hiện tốt hơn bằng sử dụng bài toán phân loại tối ưu dựa trên bổ đề “Neyman-Pearson”.

### 2.1.3. Phát hiện dựa trên phân tích tỉ lệ xám

#### 2.1.3.1. Phát biểu bài toán

Chúng ta biết rằng dù sử dụng phân hoạch (hay quyết định) nào để phân lớp ảnh có giấu tin và ảnh không có giấu tin cũng sẽ mắc phải sai số loại I với xác suất  $\alpha$  và sai số loại II với xác suất  $\beta$ . Bằng thuật toán nào thì chúng ta cũng không thể làm cực tiểu hóa xác suất của cả hai sai số này (tức là cực tiểu hóa cả  $\alpha$  và  $\beta$ ) cùng lúc mà chỉ có thể cho trước xác suất của sai số này sẽ cực tiểu hóa xác suất của sai số kia. Từ vấn đề đó đặt ra yêu cầu: Hãy xây dựng một tiêu chuẩn cho quyết định với mức  $\alpha$  cho trước và làm cực tiểu hóa  $\beta$ . Do đó để giải quyết vấn đề này luận án dựa vào bổ đề Neyman – Pearson là bổ đề cho phép tối ưu với  $\alpha$  cho trước. Áp dụng nó cho phân loại ảnh có giấu tin trên LSB của miền không gian hoặc miền tần số.

### 2.1.3.2. Phương pháp giải quyết bài toán

Trong phần này sử dụng một số bổ đề trong thống kê, từ đó có thể mở rộng các bổ đề này để có thể phân loại ảnh có giấu tin trên LSB.

*Bổ đề 2.2 (Neyman – Pearson) [108]: Cho trước  $f_0, f_1, f_2, \dots$  là những hàm khả tích đối với độ đo  $\nu$  ( $\sigma$ - hữu hạn) trên không gian  $S$ . Giả sử:*

*Tập con  $w \subset S$  và các hằng số  $c_1, c_2, c_3, \dots$  thỏa mãn:*

$$\int_w f_i(x) d\nu(x) = c_i$$

*Tập con  $w_0 \subset S$  và các hằng số  $k_1, k_2, \dots$  thỏa mãn:*

$$\begin{cases} f_0(x) \geq \sum_{i \geq 1} k_i f_i(x), x \in w_0 \\ f_0(x) < \sum_{i \geq 1} k_i f_i(x), x \notin w_0 \end{cases} \quad \text{và} \quad \int_{w_0} f_i(x) d\nu(x) = c_i \quad \text{với} \quad i = 1, 2, \dots$$

$$\text{Khi đó: } \int_{w_0} f_0(x) d\nu(x) \geq \int_w f_0(x) d\nu(x) \quad (2.4)$$

*Bổ đề 2.3 [109]: Nếu  $P(x|H_0)$  có phân bố đa thức (phân bố mũ) và giả thuyết  $H_0$  đúng thì đại lượng ngẫu nhiên:*

$$- 2 \ln \frac{P(x|H_1)}{P(x|H_0)} \text{ có phân bố } \chi^2. \quad (2.5)$$

*Bổ đề 2.4 [109, 110]: Giả sử  $f_1, f_2, \dots, f_k$  là  $k$  hàm khả tích đối với độ đo  $\mu$  nào đó ( $\sigma$ - hữu hạn) trên không gian  $S$ , còn  $A_1^*, A_2^*, \dots, A_k^*$  là một phân hoạch của  $S$  thỏa mãn điều kiện:*

$$\text{Nếu } x \in A_i^* \text{ và } f_i(x) \geq f_j(x) \text{ với } \forall j \neq i, i, j = 1, 2, \dots, k.$$

$$\text{Khi đó: } \sum_{i=1}^k \int_{A_i^*} f_i(x) d\mu(x) \geq \sum_{j=1}^k \int_{A_j} f_j(x) d\mu(x) d(x) \quad (2.6)$$

Điều này suy ra phân hoạch  $A_1^*, A_2^*, \dots, A_k^*$  là một phân hoạch tối ưu, theo nghĩa hàm lực lượng lớn nhất [108].

Đặt  $f_0(x) = P(w | H_1)$ ,  $f_1(x) = P(w | H_0)$ , khi đó  $w_0$  là miền tối ưu nếu:

$$w_0 = \{x \in \mathcal{S} : \frac{f_0(x)}{f_1(x)} \geq t(\alpha)\} \quad (2.7)$$

Hay nói cách khác:

$$w_0 = \{x \in \mathcal{S} : \frac{P(x|H_1)}{P(x|H_0)} \geq t(\alpha)\} \quad (2.7')$$

Ở đây, theo bổ đề 2.2 nếu lấy  $c_i = c = \alpha$ , ta có  $P(w_0|H_0) = \alpha$ , thì  $w_0$  được chọn như ở (2.7) hoặc (2.7') là miền làm cho xác suất (sai số loại II)  $\beta$  là bé nhất với xác suất (sai số loại I)  $\alpha$  cho trước. Còn  $t(\alpha)$  được xác định bởi bổ đề 2.3.

Để áp dụng cho việc tìm ảnh có giấu thông tin, trước hết ta giả sử  $P\{x|H_0\}$  và  $P\{x|H_1\}$  là mật độ xác suất đối với độ đo  $\mu$  ( $\sigma$ -hữu hạn) khi lần lượt giả thuyết  $H_0$ ,  $H_1$  đúng. Theo bổ đề 2.2, chúng ta phải xác định miền  $w$  sao cho:

$$\int_w p(x|H_0) d\mu(x) = \alpha \quad (0 < \alpha < 1 \text{ cho trước})$$

$$\text{và } \int_w p(x|H_1) d\mu(x) = 1 - \beta \text{ đạt giá trị lớn nhất} \quad (2.8)$$

Ứng dụng bổ đề 2.2, miền tối ưu:

$$w_0 = \{x : P(x|H_1) \geq t(\alpha) \cdot P(x|H_0)\} \text{ hay: } w_0 = \{x : \frac{P(x|H_1)}{P(x|H_0)} \geq t(\alpha)\} \quad (2.9)$$

$t(\alpha)$  được chọn sao cho  $P(w|H_0) = \alpha$

Tiếp theo chúng ta sẽ giải bài toán trong thống kê toán học sau:

**Mệnh đề 2.1:** Giả sử cho trước một đại lượng ngẫu nhiên k chiều  $X=(X_1, X_2, \dots, X_k)$  có phân bố đa thức:

$$p(X_1=r_1, X_2=r_2, \dots, X_k=r_k) = \frac{n!}{r_1! r_2! \dots r_k!} P_1^{r_1} P_2^{r_2} \dots P_k^{r_k}$$

( $r_i \geq 0$ ),  $i=1, \dots, k$ , trong đó  $n = \sum_{i=1}^k r_i$  cho trước.

Kiểm định giả thuyết  $H_0: P_1 = P_1^0, P_2 = P_2^0, \dots, P_k = P_k^0$ , ( $P_1^0, P_2^0, \dots, P_k^0$  cho trước). Đối thuyết  $H_1$ : tồn tại  $i$  để  $P_i \neq P_i^0$ .

Khi đó đại lượng ngẫu nhiên:

$$-2 \ln \lambda_{H_0} = -2n \sum_{i=1}^k \bar{P}_i \ln \frac{P_i^0}{\bar{P}_i} = -\sum_{i=1}^k 2n \frac{n P_i^0}{m_i} = \sum_{i=1}^k 2m_i \ln \frac{m_i}{n P_i^0} \quad (2.10)$$

có phân bố  $\chi^2$  với  $k-1$  bậc tự do (giả thuyết  $H_0$  đúng), với

$$\lambda_{H_0} = \left[ \left( \frac{P_1^0}{\bar{P}_1} \right)^{\bar{P}_1} \left( \frac{P_2^0}{\bar{P}_2} \right)^{\bar{P}_2} \dots \left( \frac{P_k^0}{\bar{P}_k} \right)^{\bar{P}_k} \right]^n \quad (\text{theo bổ đề 2.2, 2.3 và ước lượng hợp lý nhất})$$

trong đó  $\bar{P}_i = \frac{m_i}{n}$  ( $i=1, \dots, k$ ),  $m_i$  là tần suất xuất hiện biến cố  $i$  nào đó trong dãy  $n$  phép thử độc lập.

Chú ý: Trong thực nghiệm,  $t(\alpha)$  trong (2.9) thường được chọn là 1, và  $P_i^0$  nếu không cho trước thường được ước lượng bằng phương pháp hợp lý nhất, bằng cách ước lượng  $P_i^0$  bằng  $\bar{P}_i^0$  với  $i=1, \dots, k$ .

Do vậy công thức (2.10) có thể đơn giản thành:

$$-2 \ln \lambda_{H_0} \approx \sum_{i=1}^k 2m_i \ln \frac{\bar{P}_i}{\bar{P}_i^0} = \sum_{i=1}^k m_i 2 \ln \frac{\bar{P}_i}{\bar{P}_i^0} \quad (2.11)$$

Lúc đó đại lượng ngẫu nhiên  $\sum_{i=1}^k m_i 2 \ln \frac{\bar{P}_i}{\bar{P}_i^0}$  có phân bố  $\chi^2$  với  $k-1$  bậc tự do.

Nhưng nếu chọn  $k=1$  thì đương nhiên  $\sum m_i 2 \ln \frac{\bar{P}_i}{\bar{P}_i^0} > \ln k = \ln 1 = 0$  với  $H_0$  đúng.

Hay:

$$\left\{ \begin{array}{l} \sum_{i=1}^k m_i \ln \frac{\bar{P}_i}{P_i^0} > 0 \quad \text{nếu } H_0 \text{ đúng và} \\ \sum_{i=1}^k m_i \ln \frac{\bar{P}_i}{P_i^0} < 0 \quad \text{nếu } H_1 \text{ đúng} \\ \text{Với } \sum_{i=1}^k m_i \ln \frac{\bar{P}_i}{P_i^0} = 0 \text{ thì chưa có kết luận} \end{array} \right. \quad (2.12)$$

Đây là bài toán tối ưu theo nghĩa xác suất sai số loại I (xác suất  $\alpha$ ) cho trước, cực tiểu hoá sai số loại II (xác suất  $\beta$ ).

Áp dụng vào bài toán phát hiện ảnh có giấu tin trên LSB ta được hai phương pháp phát hiện sau đây:

### 1/. Phương pháp 1

Áp dụng bổ đề 2.2 cho phân loại tập ảnh có giấu tin trên LSB, trong trường hợp không biết trước ảnh gốc của mỗi ảnh, chúng ta phải xây dựng một ảnh làm “mốc” bằng cách tìm một ảnh có kích thước xấp xỉ (độ rộng hàng và cột, nếu tương đồng biểu đồ tần suất càng tốt) ảnh cần phân loại.

Sử dụng hệ thức (2.12) (được xây dựng từ bổ đề 2.2) làm cơ sở cho việc phát hiện ảnh có hay không giấu thông tin trên LSB. Trong ứng dụng thực tế, nếu  $\bar{P}_i \neq \bar{P}_i^0$  thì việc kiểm định giả thiết mới có ý nghĩa. Mặc dù vậy có thể  $\bar{P}_i \neq \bar{P}_i^0$  với  $\forall i$ , (nếu  $\exists i: \bar{P}_i = \bar{P}_i^0$  thì loại ra khỏi công thức), nhưng sự khác biệt không lớn lắm. Trường hợp như vậy, hệ thức (2.12) để kiểm định giả thuyết  $H_0$  cho độ chính xác không cao. Do đó, khi áp dụng vào việc phát hiện ảnh có hay không giấu thông tin trên LSB, luận án đã cải tiến như sau:

Chúng ta biết rằng do tính chất của logarit với  $\forall t$ , ta đều có:  $t \cdot \ln \frac{\bar{P}_1}{P_1^0} = \ln \left( \frac{\bar{P}_1}{P_1^0} \right)^t$ . Do đó nếu chọn  $t \geq 2$  thì  $\left( \frac{\bar{P}_1}{P_1^0} \right)^t$  sẽ tăng hoặc giảm lên  $t$  lần tùy theo  $\frac{\bar{P}_1}{P_1^0} > 1$

hay  $\frac{\bar{P}_1}{P_1^0} < 1$ . Với  $t$  càng lớn thì sự khuếch đại càng lớn khi  $\frac{\bar{P}_1}{P_1^0} > 1$ , ngược lại khi  $\frac{\bar{P}_1}{P_1^0} < 1$ .

Thực tế giá trị của  $t$  phụ thuộc vào kích thước của ảnh, kích thước ảnh càng lớn,  $t$  càng lớn sao cho nó có khả năng phân loại tốt.

#### *Cách phát hiện khi không có ảnh gốc*

Giả sử có một ảnh bất kỳ  $Z$ , kiểm tra xem ảnh  $Z$  có giấu tin trên LSB hay không.

Khi không có ảnh gốc để kiểm tra chúng ta phải chọn một ảnh làm “mốc” như sau: chọn một ảnh gốc  $U$  có kích thước  $n = p * q$  xấp xỉ ảnh  $Z$ , tính tần suất các điểm ảnh được vector  $X = \{x_i, i = 0, \dots, 255\}$ . Đặt  $\bar{P}_i^0 = \frac{x_i}{n}$  với  $i = 0, \dots, 255$ .

Nhúng thông tin vào LSB của ảnh  $U$  theo thuật toán giấu LSB ngẫu nhiên với tỷ lệ bit giấu là 100% trên miền LSB được ảnh  $S$  có giấu thông tin.

Ký hiệu  $\bar{P}_i = \frac{y_i}{n}$  ( $y_i$  là tần suất xuất hiện điểm ảnh  $i$  trong ảnh stego  $S$ ).

Tiếp theo lập vector  $C = \{c_i, c_i = \lceil t \cdot \ln \frac{\bar{P}_i}{P_1^0} \rceil, i = 0, \dots, 255\}$  (2.13)

( $\lceil x \rceil$  là phần nguyên của  $x$ ).

Giá trị  $t$  được chọn sao cho:  $\max\{c_i\} - \min\{c_i\} \geq 400, i = 0, \dots, 255$ . Việc lựa chọn này dựa trên đánh giá trên cùng một tập ảnh (gồm 500 ảnh) với các giá trị  $t$  khác nhau, để có được giá trị  $t$  phù hợp việc lựa chọn như  $\chi_1^2(\alpha)$  trong 2.1.2.2.

Tính tần suất điểm ảnh của  $Z$  (ảnh cần kiểm tra) được vector  $F = \{f_1, f_2, \dots, f_{255}\}$ . Lập tích vô hướng:

$$c\_f = \sum_{i=0}^{255} c_i f_i, \text{ (với } c_i \text{ tính theo (2.13))} \quad (2.14)$$

Nếu  $c\_f > 0$ , kết luận  $Z$  là ảnh có giấu tin trên LSB

Nếu  $c_f < 0$ , kết luận  $Z$  là không giấu tin trên LSB

Nếu  $c_f = 0$ , thì chưa có kết luận.

Vậy trong trường hợp chúng ta không biết trước ảnh gốc của ảnh cần kiểm tra, ta phải xây dựng một ảnh có kích cỡ xấp xỉ (nếu tương đồng biểu đồ tần suất càng tốt) ảnh cần phân loại. Sau đó ảnh này được nhúng với tỉ lệ 100% LSB của ảnh. Từ đó chúng ta có thể xây dựng phương pháp nhận dạng theo tỉ lệ xấp xỉ nhất như sau:

### **Thuật toán 2.3 – Thuật toán “Tỉ lệ xấp xỉ 1”**

**Đầu vào:** Cho tập ảnh 8-bit màu  $\mathcal{J}$  bất kỳ (gồm giấu tin trên LSB và ảnh gốc).

**Đầu ra:** Phân tập đó thành tập  $\mathcal{S}$  (ảnh có giấu trên LSB) và  $\mathcal{C}$  (ảnh không giấu trên LSB).

*Các bước thực hiện:*

**Bước 1:** Phân tập ảnh  $\mathcal{J}$  thành từng nhóm có kích cỡ xấp xỉ nhau.

Mỗi nhóm thực hiện theo bước 2, 3 cho đến khi hết các nhóm ảnh.

**Bước 2:** Mỗi nhóm dựng một ảnh gốc  $C$  (bất kỳ) có kích cỡ bằng kích cỡ của nhóm.

Ảnh  $C$  được nhúng lượng thông tin vào các bit LSB với tỉ lệ 100% tổng số LSB của ảnh. Lập vector  $c$  theo (2.13).

**Bước 3:** Mỗi ảnh thuộc nhóm đang xét thực hiện tính theo (2.14), ta nhận được giá trị  $c_f$ . Nếu  $c_f > 0$  thì bổ sung ảnh đang xét vào tập  $\mathcal{S}$ , nếu  $c_f < 0$  thì bổ sung ảnh vào tập  $\mathcal{C}$ . Nếu  $c_f = 0$  thì loại ra ngoài tập không xét (trong thực nghiệm hiếm khi thấy  $c_f = 0$ ).

Ví dụ: Giả sử có hai ảnh phong cảnh cấp xám image01.bmp kích cỡ 768x512 điểm ảnh (hình 2.1 a), và image02.bmp kích cỡ 760x520 (hình 2.1 b).





Hình 2.1: Ảnh thử nghiệm cho kỹ thuật “tỉ lệ xám 1”

Hai ảnh được giấu lượng bit thông tin với tỉ lệ từ 10% đến 100% (mỗi lần tăng lên 10%) ta được một tập gồm 22 ảnh (20 ảnh đã giấu tin và 2 ảnh gốc). Hãy phân loại tập 22 ảnh này thành hai tập gốc và tập ảnh có giấu tin trên LSB.

Vì tập ảnh có kích thước xấp xỉ nhau, nên ta chọn image01.bmp và fimage01100.bmp (ảnh image01.bmp được nhúng thông tin trên 100% LSB của ảnh) làm ngưỡng để tính được  $c_i$  ( $i = 0, \dots, 255$ ) theo (2.13).

Sau đó thực hiện tính tiếp  $c_f$  theo (2.14) cho 22 ảnh trong tập ảnh, ta được kết quả theo bảng 2.6.

Bảng 2.6: Kết quả thử nghiệm đánh giá  $c_f$  theo (2.14)

| Lượng tin giấu (%) | image01.bmp<br>được ( $c_f$ ) | image02.bmp<br>được ( $c_f$ ) |
|--------------------|-------------------------------|-------------------------------|
| 0                  | -21742491                     | -65471394                     |
| 10                 | -13548708                     | -49278151                     |
| 20                 | -6142813                      | -34649430                     |
| 30                 | 453826                        | -21612223                     |
| 40                 | 6556129                       | -9556037                      |
| 50                 | 12171845                      | 1538080                       |
| 60                 | 17209329                      | 11486152                      |
| 70                 | 21631144                      | 20230689                      |
| 80                 | 25626185                      | 28119354                      |
| 90                 | 29221022                      | 35218561                      |
| 100                | 32597198                      | 41881232                      |

Từ bảng 2.6 ta thấy với tập ảnh tạo ra từ image01.bmp có thể dùng (2.14) để phát hiện cho chính nó với tỉ lệ giấu từ 30% trở lên, với tập ảnh tạo ra từ ảnh

image02.bmp phát hiện khi giấu từ 50% trở lên, vì ảnh này có kích cỡ xấp xỉ với ảnh image01.bmp.

## 2/. Phương pháp 2

Phương pháp thứ 2 phân loại ảnh theo công thức (2.11) như sau:

$T = \sum_{i=1}^n 2m_i \ln \frac{m_i}{nP_i^0}$  có phân bố  $\chi^2$  với n-1 bậc tự do khi giả thuyết  $H_0$  đúng, tức là có xác suất:

$$P(T \geq t_0) = \int_{t_0}^{\infty} p_n(t) dt$$

Trong đó  $p_n(t)$  là hàm mật độ xác suất. Ta có thể xác định được ngưỡng  $t_0$  qua phương trình sau:

$$\alpha_0 = \int_{t_0}^{\infty} p_n(t) dt = 1 - \int_{-\infty}^{t_0} p_n(t) dt$$

Nếu biết được n và  $\alpha = \alpha_0$ , ta có thể xác định được  $t_0$  bằng cách tra bảng  $\chi^2$  trong [108, 109] với n = 256, độ tin cậy  $\alpha = 0.1$ , ta được  $t_0=284.3359$ .

*Áp dụng giải bài toán phát hiện như sau:*

Chọn một ảnh gốc C bất kỳ từ tập  $C_0$  có kích thước n = p \* q, thống kê tần suất các điểm ảnh được vector  $X = \{x_i, i=0, \dots, 255\}$ . Đặt  $\bar{P}_i^0 = \frac{x_i}{n}$  với  $i=0, \dots, 255$ .

Sử dụng thuật toán giấu tin LSB ngẫu nhiên để tạo ra 11 ảnh có giấu tin trên LSB, ký hiệu  $S_0, \dots, S_{10}$ , có tỉ lệ giấu trên miền LSB từ 0 % đến 100 % (mỗi lần tăng lên 10%). Sau đó mỗi ảnh  $S_j$  ( $j=0, \dots, 10$ ) ta cũng thống kê tần suất điểm ảnh của ảnh được vector  $Y = \{y_i, i=0, \dots, 255\}$ . Đặt  $\bar{P}_i = \frac{y_i}{n}$  với  $i=0, \dots, 255$ .

Áp dụng công thức (2.11) ta được  $T = \sum_{i=0}^{255} 2x_i \ln \frac{\bar{P}_i}{\bar{P}_i^0}$  cho mỗi cặp ảnh (C, stego\_j,  $j=0, \dots, 10$ ) ta được kết quả trong bảng 2.7.

**Bảng 2.7: Kết quả thử nghiệm đánh giá T theo (2.11)**

| <b>Ảnh S<sub>i</sub> (i = 0,.., 10)</b> | <b>T của cặp (C, S<sub>i</sub>)</b> |
|---|-------------------------------------|
| 0                                       | 0                                   |
| 1                                       | 159.40                              |
| 2                                       | 454.30                              |
| 3                                       | 807.00                              |
| 4                                       | 924.60                              |
| 5                                       | 1064.80                             |
| 6                                       | 1020.20                             |
| 7                                       | 1167.40                             |
| 8                                       | 1279.10                             |
| 9                                       | 1352.20                             |
| 10                                      | 1660.80                             |

*Phát hiện khi không có ảnh gốc*

Theo [95] trên các ảnh giấu tin bằng kỹ thuật LSB, các cặp giá trị PoV ( $x_{2i}$ ,  $x_{2i+1}$ ),  $i=0, \dots, 127$  có giá trị càng gần nhau khi lượng thông tin giấu xấp xỉ 100%. Khi không có ảnh gốc để so sánh, chúng ta có thể coi ảnh “mốc” để so sánh là ảnh được giấu 100% trên miền LSB, tức là  $x_{2i} \approx x_{2i+1} = \frac{x_{2i} + x_{2i+1}}{2}$ . Khi đó giá trị T sẽ thay đổi như bảng 2.8.

**Bảng 2.8: Kết quả thử nghiệm đánh giá T sau khi ước lượng ảnh “mốc”**

| <b>Ảnh S<sub>i</sub> (i = 0,.., 10)</b> | <b>Giá trị T của cặp (ảnh “mốc”, S<sub>i</sub>)</b> |
|---|---|
| 0                                       | 1477.20   |
| 1                                       | 1537.90   |
| 2                                       | 749.90  |
| 3                                       | 587.70  |
| 4                                       | 496.80  |
| 5                                       | 485.00  |
| 6                                       | 427.90  |
| 7                                       | 357.10  |
| 8                                       | 228.80  |
| 9                                       | 172.40  |
| 10                                      | 133.80  |

Từ đó chúng ta đưa ra thuật toán tổng quát theo phương pháp 2 sau đây.

### **Thuật toán 2.4 – Thuật toán “Tỉ lệ xám 2”**

**Đầu vào:** Cho tập ảnh 8-bit cấp độ xám  $\mathcal{V}$  bất kỳ (gồm ảnh có giấu tin và ảnh gốc)

**Đầu ra:** Phân loại tập  $\mathcal{V}$  thành tập  $\mathcal{S}$  (ảnh có giấu trên LSB) và tập  $\mathcal{C}$  (ảnh gốc).

*Các bước thực hiện*

**Bước 1:** Chọn lần lượt từng ảnh  $I$  có kích cỡ  $p * q$  trong tập  $\mathcal{V}$ , sau đó thực hiện các bước 2 và 3 cho đến khi xét hết các ảnh đầu vào.

**Bước 2:** Thống kê tần suất điểm ảnh của ảnh  $I$  được vector  $X = \{x_i, i=\overline{0, 255}\}$  với  $x_i$  là tần suất của điểm ảnh có giá trị  $i$ . Thực hiện tính  $P_i^0$  với

$$P_{2j}^0 = P_{2j+1}^0 = \frac{x_{2j} + x_{2j+1}}{2pq} \quad (j=0, \dots, 127). \text{ Áp dụng công thức (2.11) ta có:}$$

$$T = \sum_{i=0}^{255} 2x_i \ln \frac{x_i}{(pq)P_i^0}$$

**Bước 3:** Chọn ngưỡng  $t_0$ . Nếu  $T > t_0$ , thì  $I$  lưu vào tập  $\mathcal{C}$ , ngược lại  $I$  lưu vào tập  $\mathcal{S}$ .

Dựa trên thử nghiệm với một tập ảnh lớn (2000 ảnh), chọn  $t_0 = 500$  cho kết quả phân loại tốt.

#### **2.1.4. Phát hiện bằng phương pháp ước lượng thông tin giấu trên LSB**

Ba phương pháp phát hiện mù ở trên chủ yếu đưa ra phương pháp kết luận một ảnh bất kỳ có giấu tin trên LSB hay không, nếu ảnh được xét kết luận là có giấu tin chúng ta chưa biết nó được giấu với tỉ lệ bit giấu là bao nhiêu phần trăm miền LSB của ảnh. Do đó để ước lượng xấp xỉ số bit thông tin giấu, trong chương này đưa ra một phương pháp ước lượng dựa trên lý thuyết trùng khớp. Đầu tiên chúng ta sẽ thực hiện ước lượng khi có ảnh gốc. Trong trường hợp không có ảnh gốc chúng ta phải ước lượng xấp xỉ một ảnh làm “mốc” từ ảnh cần kiểm tra.

### 2.1.4.1. Phương pháp ước lượng khi có ảnh gốc

Phương pháp ước lượng độ dài thông tin giấu trên miền LSB dựa trên lý thuyết trùng khớp sau đây.

Giả sử  $X_0=(x_{0,0}, x_{0,1}, \dots, x_{0,n-1})$ ,  $X_1=(x_{1,0}, x_{1,1}, \dots, x_{1,n-1})$  là hai vector ngẫu nhiên độc lập nhau, có phân bố xác suất lần lượt là  $P_0(t)$ ,  $P_1(t)$  trong đó:

$$P_j(t) = P(X_{j,i}=t), j=0,1; \quad i=\overline{0, n-1}; \quad 0 \leq t \leq m-1$$

Trường hợp  $X_0, X_1$  cùng phân bố, thì ta có  $p_0(t) = p_1(t)$ .

Khi đó ta nói rằng hai vector  $X_0$  và  $X_1$  có sự trùng khớp (coincidence) tại vị trí thứ  $i$  nếu tại đó  $x_{0,i} = x_{1,i}$ .

Đặt:

$$\chi_0^1(i) = \begin{cases} 1 & \text{nếu } x_{0,i} = x_{1,i} \\ 0 & \text{nếu } x_{0,i} \neq x_{1,i} \end{cases}$$

Ký hiệu  $\theta(X_0, X_1)$  là số những trùng khớp giữa hai vector  $X_0, X_1$ , khi đó:

$$\theta(X_0, X_1) = \sum_{i=1}^{n-1} \chi_0^1(i)$$

*Định lý 2.4:* Cho  $X_0, X_1$  là hai đại lượng ngẫu nhiên độc lập nhau, có phân bố là  $p_0(t), p_1(t)$  tương ứng, khi đó:

$$P(X_{0,i}=X_{1,i}) = \sum_{t=0}^{m-1} P_0(t).P_1(t) \quad (2.15)$$

Chứng minh:

Ta có biến cố  $(X_{0,i}=X_{1,i}) = \cup_{t=0}^{m-1} (X_{0,i} = X_{1,i} = t)$ . Đây là hợp của  $m$  biến cố rời nhau. Do đó xác suất của biến cố  $\{X_{0,i}=X_{1,i}\}$  là:

$$P(X_{0,i}=X_{1,i}) = P \cup_{t=0}^{m-1} (X_{0,i} = X_{1,i} = t) = \sum_{t=0}^{m-1} P(X_{0,i} = X_{1,i} = t)$$

Do tính độc lập ta suy ra:  $P(X_{0,i}=t, X_{1,i}=t) = P(X_{0,i}=t).P(X_{1,i}=t) = P_0(t).P_1(t)$

Vậy  $P(X_{0,i}=X_{1,i}) = \sum_{t=0}^{m-1} p_0(t)p_1(t)$  (điều phải chứng minh)

Để ứng dụng định lý 2.4 vào bài toán ước lượng độ dài thông tin nhúng trong ảnh số, ta cần phải xác định được  $P_0(t)$ ,  $P_1(t)$  trong trường hợp  $m = 2$ , tức là  $t$  chỉ nhận một trong hai giá trị 0 hoặc 1.

Để đơn giản ta xét ngôn ngữ của thông tin được nhúng là tiếng Anh. Từ thống kê trong [20] trên 10000 ký tự các văn bản tiếng Anh chính thống, tần suất đơn các ký tự trong văn bản tiếng Anh tự nhiên xuất hiện không đều. Trong đó ký tự e xuất hiện nhiều nhất (chiếm 12.9%) so với tổng số các ký tự xuất hiện trong văn bản. Còn chữ z xuất hiện rất ít (chiếm 0.05%). Theo [20] có kết quả thống kê tần suất các chữ cái trong văn bản tiếng Anh theo bảng 2.9 (không phân biệt chữ hoa chữ thường).

**Bảng 2.9. Bảng thống kê tần suất xuất hiện của các chữ cái trong văn bản tiếng Anh**

| Ký tự | Tần suất xuất hiện | Mã nhị phân | Ký tự | Tần suất xuất hiện | Mã nhị phân |
|-------|--------------------|-------------|-------|--------------------|-------------|
| a     | 7.96               | 01100001    | n     | 7.51               | 01101110    |
| b     | 1.60               | 01100010    | o     | 6.62               | 01101111    |
| c     | 2.84               | 01100011    | p     | 1.81               | 01110000    |
| d     | 4.01               | 01100100    | q     | 0.17               | 01110001    |
| e     | 12.86              | 01100101    | r     | 6.83               | 01110010    |
| f     | 2.62               | 01100110    | s     | 6.62               | 01110011    |
| g     | 1.99               | 01100111    | t     | 9.72               | 01110100    |
| h     | 5.39               | 01101000    | u     | 2.48               | 01110101    |
| i     | 7.77               | 01101001    | v     | 1.15               | 01110110    |
| j     | 0.16               | 01101010    | w     | 1.80               | 01110111    |
| k     | 0.41               | 01101011    | x     | 0.17               | 01111000    |
| l     | 3.51               | 01101100    | y     | 1.52               | 01111001    |
| m     | 2.43               | 01101101    | z     | 0.05               | 01111010    |

Từ bảng 2.9 ta thấy giá trị trung bình chữ số “0” xuất hiện trong văn bản tùy ý xấp xỉ bằng  $E[X = 0] = 2.4912$  nếu đem chia cho 8 (độ dài bit của các ký tự chữ cái) ta có  $E[X = 0]/8 = 0.3114$ . Đây chính là xác suất để chữ số “0” xuất hiện trong văn bản tiếng Anh dưới dạng nhị phân tức là  $P_0(t = 0) = 0.3114$  và xác suất để chữ số “1” xuất hiện là  $P_0(t = 1) = 1 - 0.3114 = 0.6886$ .

Xác suất để chữ số “0” và chữ số “1” xuất hiện trên các bit LSB của ảnh là  $P_1(t = 0)$  và  $P_1(t = 1)$  được ước lượng bằng phương pháp hợp lý cực đại cho ta kết quả như sau:  $P_1(t = 0) \approx 0.505$ ,  $P_1(t = 1) \approx 0.495$ .

Vậy xác suất xuất hiện trùng khớp giữa bit thông tin và bit LSB của ảnh gốc là:

$$P_0(t=0) * P_1(t=0) + P_0(t=1) * P_1(t=1) = 0.3114 * 0.505 + 0.6886 * 0.495 = 0.498114 \approx 0.5 = \frac{1}{2}.$$

Giả sử ta có chuỗi các bit bản rõ là  $X = x_0x_1x_2\dots x_{n-1}$  với  $x_i \in \{0, 1\}$  và dãy các bit LSB của ảnh (ảnh cấp xám 8 - bit hoặc ảnh 24 - bit màu) là  $Y = y_0y_1y_2\dots y_{n-1}$  với  $y_i \in \{0, 1\}$ .

Theo định lý 2.4 trên ta có  $P\{x_i = y_i\} \approx 1/2$ , vì độ dài bản thông tin tính theo bit là  $n$ , nên số các điểm ảnh không bị đảo bit (bitwise) ở LSB sẽ xấp xỉ là  $n/2$ . Như vậy nếu ta ước lượng được số điểm ảnh bị đảo bit là bao nhiêu thì ta có thể ước lượng xấp xỉ được độ dài bản thông tin được giấu trong ảnh.

Để ước lượng độ dài thông tin giấu trong LSB của ảnh, thực hiện khảo sát sau: Có 2 ảnh gốc là  $C_1$  và  $C_2$ , hai ảnh này được giấu tin với tỉ lệ lần lượt là 12% và 9% (so với kích cỡ của  $C_1$  và  $C_2$ ) được ảnh stego  $S_1$  và  $S_2$ . Sau khi thống kê tần suất các điểm ảnh của từng cặp ảnh ( $C_i, S_i$ ),  $i=\{1, 2\}$ , lưu vào các cặp vector ( $C_i^{256}, S_i^{256}$ ), tính hiệu  $|c_i^{(j)} - s_i^{(j)}|$ ,  $j=0, \dots, 255$ , ta có kết quả theo bảng 2.10.

**Bảng 2.10. Thử nghiệm độ chênh lệch  $|c_i^j - s_i^j|$  của ảnh có giấu tin và ảnh gốc**

| <b>j</b> | <b><math>c_1^j</math></b> | <b>s</b> | <b><math> c_1^j - s_1^j </math></b> | <b><math>c_2^j</math></b> | <b><math>s_2^j</math></b> | <b><math> c_2^j - s_2^j </math></b> |
|----------|---------------------------|----------|-------------------------------------|---------------------------|---------------------------|-------------------------------------|
| 0        | 1615                      | 1014     | 601                                 | 1989                      | 1910                      | 79                                  |
| 1        | 673                       | 790      | 117                                 | 551                       | 542                       | 9                                   |
| 2        | 421                       | 489      | 68                                  | 373                       | 345                       | 28                                  |
| 3        | 386                       | 418      | 32                                  | 316                       | 281                       | 35                                  |
| 4        | 433                       | 413      | 20                                  | 310                       | 329                       | 19                                  |
| 6        | 411                       | 412      | 1                                   | 306                       | 316                       | 10                                  |
| 6        | 417                       | 394      | 23                                  | 303                       | 326                       | 23                                  |
| 7        | 505                       | 510      | 5                                   | 407                       | 403                       | 4                                   |
| 8        | 549                       | 585      | 36                                  | 476                       | 479                       | 3                                   |
| 9        | 546                       | 568      | 22                                  | 509                       | 524                       | 15                                  |
| ...      | ...                       | ...      | ...                                 | ...                       | ...                       | ...                                 |
| 255      | 39                        | 60       | 21                                  | 1149                      | 1750                      | 601                                 |
| $\Sigma$ |                           | 393216   | 15220                               |                           | 393216                    | 11174                               |

Rõ ràng nếu  $s_i^j = c_i^j$ , tức là không nhúng thông tin hay  $|s_i^j - c_i^j| = 0$ . Ngược lại,  $|s_i^j - c_i^j| > 0$  là do lượng tin được nhúng vào trong  $C_i$  đã làm cho các điểm ảnh có sự thay đổi. Mỗi điểm ảnh cùng lắm chỉ nhúng được một bit thông tin, do đó tổng  $\sum_{j=0}^{255} |c_i^j - s_i^j|$  chính là số các bit thông tin đã được nhúng.

Nếu gọi  $n_i$  là độ dài bit thông tin đã được nhúng trong ảnh gốc  $C_i$  thì theo định lý 2.4, ta có ước lượng:

$$n_i - \frac{n_i}{2} \approx \sum_{j=0}^{255} |c_i^j - s_i^j| \Leftrightarrow n_i \approx 2 \sum_{j=0}^{255} |c_i^j - s_i^j| = N_i \quad (2.16)$$

Nếu cho trước ảnh gốc và ảnh có giấu thông tin tương ứng, chúng ta có thể ước lượng được số bit thông tin đã được nhúng trong ảnh.

Xét lại ví dụ trên, áp dụng (2.16) với cặp  $(C_1, S_1)$  ta được:

$$2 \sum_{j=0}^{255} |c_1^j - s_1^j| = 30440$$

Vậy độ dài thông tin nhúng trong  $S_1$  là  $n_1 \approx 30440$  chiếm tỉ lệ (so với kích cỡ của ảnh) là  $\frac{30440}{393216} \approx 7.74\%$

Với cặp ảnh  $(C_2, S_2)$  ta có  $2 \sum_{j=0}^{255} |c_2^j - s_2^j| = 22348$ , chiếm tỉ lệ  $\frac{22348}{393216} \approx 5.68\%$ .

Vấn đề đặt ra ở đây là một số trường hợp trong thực tế chúng ta không biết trước ảnh gốc mà chỉ biết ảnh quan sát, chúng ta phải tìm cách xây dựng một ảnh làm “mốc” từ ảnh quan sát đã biết.

#### **2.1.4.2. Phương pháp ước lượng không dựa vào ảnh gốc**

Khi không có ảnh gốc chúng ta cần phải xây dựng một ảnh làm “mốc” từ một ảnh được xét. Theo [95] sau khi nhúng chuỗi bit thông tin với tỉ lệ 100% trên miền LSB của ảnh  $C$  (xấp xỉ 12.5% kích cỡ của ảnh), thì giá trị tần suất của các cặp PoV  $(x_{2i}, x_{2i+1})$  xấp xỉ bằng nhau. Từ đó luận án đưa ra ý tưởng sau:



Một ảnh bất kỳ S với vector tần suất điểm ảnh  $X=\{x_0, x_1, x_2, \dots, x_{255}\}$ , ta có thể ước lượng được vector tần suất điểm ảnh  $Y=\{y_0, y_1, \dots, y_{255}\}$  của ảnh làm “mốc” với:

$$y_{2i} = y_{2i+1} = \frac{x_{2i} + x_{2i+1}}{2}, i=0, \dots, 127 \quad (2.17)$$

Sau đó ta có thể ước lượng xấp xỉ tỉ lệ thông tin giấu trong ảnh S (kích cỡ  $p \times q$  điểm ảnh) theo công thức sau:

$$L = \frac{pq}{8pq} 100 - \left[ \frac{1}{pq} \sum_{i=0}^{255} \text{abs}(x_i - y_i) \right] \cdot 100 \quad (2.18)$$

Nếu ảnh có giấu tin thì giá trị của  $|x_i - y_i|$  tiến tới 0 và L tiến tới 12.5. Còn trường hợp ảnh là ảnh gốc thì  $\left[ \frac{1}{pq} \sum_{i=0}^{255} \text{abs}(x_i - y_i) \right] \cdot 100$  tiến tới 12.5 và L tiến tới 0.

Giả sử ta có một ảnh  $C_1$  (ảnh gốc) với vector tần suất điểm ảnh tương ứng  $X_1^{256}$ , và ảnh  $S_1$  (ảnh có giấu tin được nhúng với tỉ lệ bit thông tin bằng 100% miền LSB của ảnh gốc) với vector tần suất tương ứng  $X_2^{256}$ . Áp dụng (2.17) ta có vector tần suất điểm ảnh xấp xỉ  $Y_1^{256}$  và  $Y_2^{256}$ , từ  $X_1^{256}$  và  $X_2^{256}$  tính hiệu  $|x_i^j - y_i^j|$ ,  $j=0, \dots, 255$ ,  $i=1, 2$  ta có kết quả theo bảng 2.11.

**Bảng 2.11. Độ sai lệch giữa tần suất của ảnh kiểm tra và ảnh ước lượng làm “mốc”**

| j        | $x_1^j$ | $y_1^j$ | $ x_1^j - y_1^j $ | $x_2^j$ | $y_2^j$ | $ x_2^j - y_2^j $ |
|----------|---------|---------|-------------------|---------|---------|-------------------|
| 0        | 1014    | 1597    | 583               | 1615    | 1597    | 18                |
| 1        | 790     | 687     | 103               | 673     | 687     | 14                |
| 2        | 489     | 431     | 58                | 421     | 431     | 10                |
| 3        | 418     | 396     | 22                | 386     | 396     | 10                |
| 4        | 413     | 419     | 6                 | 433     | 419     | 14                |
| 6        | 412     | 419     | 7                 | 411     | 419     | 8                 |
| 6        | 394     | 412     | 18                | 417     | 412     | 5                 |
| 7        | 510     | 495     | 15                | 505     | 495     | 10                |
| 8        | 585     | 555     | 30                | 549     | 555     | 6                 |
| 9        | 568     | 563     | 5                 | 546     | 563     | 17                |
| ...      | ...     | ...     | ...               | ...     | ...     | ...               |
| 255      | 60      | 36      | 24                | 39      | 36      | 3                 |
| $\Sigma$ | 393216  |         | 13082             | 393216  |         | 4670              |

Ta tính được giá trị ước lượng xấp xỉ cho ảnh  $C_1$  và  $S_1$  lần lượt  $L_1, L_2$  với  $L_1 = 3.846151, L_2 = 10.12472$ .

Thực tế, ảnh khi giấu thông tin với tỉ lệ giấu trên 100% LSB của ảnh không hoàn toàn làm cho  $y_{2i} = y_{2i+1} = (x_{2i} + x_{2i+1})/2$ , vì vậy (2.18) được thay đổi với sai số  $\Delta x$  như sau:

$$L = \frac{pq}{8pq} \cdot 100 - \left( \frac{1}{pq} \sum_{i=0}^{255} \text{abs}(x_i - y_i) \right) \cdot 100 - \Delta x \quad (2.19)$$

Dựa vào thực nghiệm có thể chọn  $\Delta x = 3.5$  cho kết quả tốt.

Biểu thức (2.19) chỉ ước lượng được lượng thông tin giấu theo tỉ lệ so với kích thước ảnh. Một số kỹ thuật ước lượng khác tính lượng thông tin giấu theo tỉ lệ 0%, 10%, 20%, ..., 100% so với kích thước miền LSB của ảnh. Vì vậy dựa trên thực nghiệm sau ta sẽ xây dựng biểu thức chuyển đổi tương ứng từ biểu thức (2.19).

Khảo sát trên một tập 10 ảnh chuẩn cấp xám 8 bit (hình 2.2) cùng kích cỡ 512x512 tải về từ [107].



Hình 2.2. Tập 10 ảnh chuẩn lấy về từ [107]

Thực hiện giấu thông tin bằng kỹ thuật giấu LSB trên tập ảnh này với tỉ lệ giấu 0%, 10%, .. 100%. Thực hiện ước lượng cho từng tập ảnh ta được giá trị ước lượng cho trong bảng 2.12.

**Bảng 2.12. Kết quả ước lượng xấp xỉ trung bình thông tin giấu trên LSB với tập 10 ảnh**

| Lượng thông tin tin đã giấu (%) | Lượng thông tin ước lượng trung bình trên tập 10 ảnh (%) |
|---------------------------------|--|
| 0                               | 0  |
| 10                              | 0.07   |
| 20                              | 0.23645  |
| 30                              | 0.47601  |
| 40                              | 0.80586  |
| 50                              | 1.4977   |
| 60                              | 1.9002   |
| 70                              | 2.6901   |
| 80                              | 4.0328   |
| 90                              | 5.738  |
| 100                             | 6.6821   |

Từ đó chúng ta xây dựng được phương trình bậc hai ước lượng xấp xỉ từ bảng 2.12 như sau:

$$-3.54x^2 + 38.64x = y \quad (2.20)$$

Do đó, ứng với mỗi giá trị L tìm được từ (2.19) của ảnh, thay  $x = L$  vào (2.20), sẽ nhận được y tương ứng chính là lượng thông tin xấp xỉ đã giấu trên LSB của ảnh. Bảng 2.13 là kết quả ước lượng xấp xỉ theo (2.20) từ bảng kết quả 2.12.

**Bảng 2.13. Kết quả ước lượng xấp xỉ theo (2.19) và (2.20) trên tập 10 ảnh chuẩn**

| Lượng tin giấu (%) | Tỉ lệ ước lượng xấp xỉ trung bình (%) |                       |
|--------------------|---------------------------------------|-----------------------|
|                    | Theo biểu thức (2.19)                 | Theo biểu thức (2.20) |
| 0                  | 0                                     | 0                     |
| 10                 | 0.07                                  | 2.6875                |
| 20                 | 0.23645                               | 8.9385                |
| 30                 | 0.47601                               | 17.591                |
| 40                 | 0.80586                               | 28.84                 |
| 50                 | 1.4977                                | 49.931                |
| 60                 | 1.9002                                | 60.642                |
| 70                 | 2.6901                                | 78.328                |
| 80                 | 4.0328                                | 98.255                |
| 90                 | 5.738                                 | 99.75                 |
| 100                | 6.6821                                | 100                   |

Từ biểu thức (2.19) và (2.20) chúng ta xây dựng thuật toán ước lượng thông tin tổng quát trên miền LSB của ảnh như sau:

## **Thuật toán 2.5 – Ước lượng tỉ lệ thông tin giấu trên LSB của ảnh**

**Đầu vào:** Một ảnh 8 – bit cấp độ màu C

**Đầu ra:** Cho biết tỉ lệ bit thông tin giấu trên LSB miền không gian của ảnh

**Bước 1.** Tính tần suất của dữ liệu ảnh C được vector tương ứng  $X^{256}$ .

**Bước 2.** Áp dụng (2.18) ta có vector tần suất điểm ảnh  $Y^{256}$  cho ảnh làm “mốc” được giấu tỉ lệ 100% trên miền LSB.

**Bước 3.** Áp dụng (2.19) được lượng thông tin L (tính theo tỉ lệ so với kích cỡ ảnh)

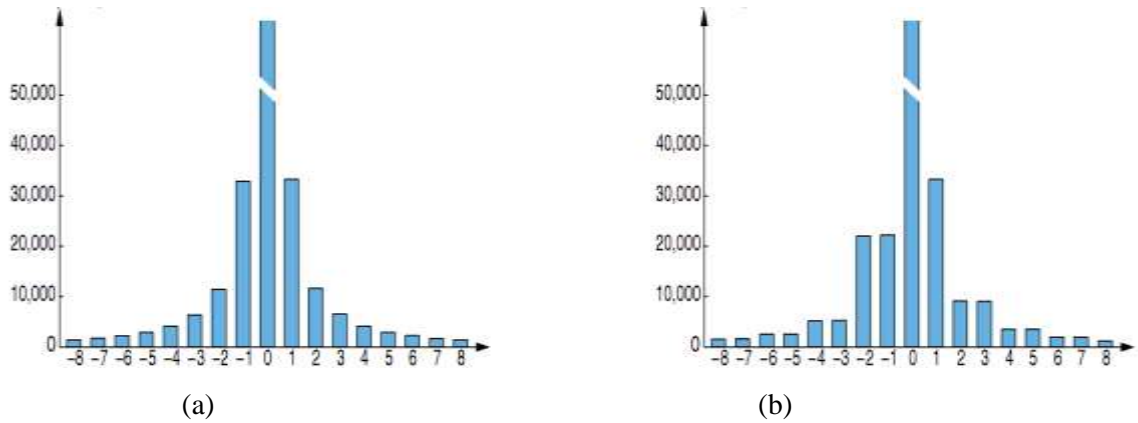
**Bước 4.** Thay  $x = L$  vào (2.20), sẽ nhận được lượng thông tin xấp xỉ đã giấu trên LSB của ảnh (tính theo tỉ lệ so với kích cỡ miền LSB của ảnh).

## **2.2. KỸ THUẬT PHÁT HIỆN MÙ TRÊN LSB CỦA MIỀN TẦN SỐ**

### **2.2.1. Phân tích kỹ thuật giấu LSB trên miền tần số**

Giấu tin trên miền tần số cosine hay wavelet là hình thức giấu tin trên LSB của các hệ số cosine trên miền tần số giữa như các kỹ thuật [23, 69, 70, 94, 104] hay trên các băng tần cao LH, HL, HH như các kỹ thuật [42, 73, 91]. Phương pháp biến đổi miền không gian sang miền tần số cosine (wavelet) như đã giới thiệu trong chương 1. Theo nhận định của các nhà giấu tin phương pháp giấu trên các hệ số này không làm ảnh hưởng đến chất lượng ảnh.

Theo Provos và các cộng sự, kỹ thuật giấu thông tin trên LSB của các hệ số cosine cũng gây ra cân bằng các cặp PoV của hệ số cosine [71]. Theo minh họa trong hình 2.3 về biểu đồ tần suất các hệ số cosine trên ảnh Lena.bmp trước khi giấu tin (hình 2.3 (a)) và ảnh sau khi giấu tin trên các hệ số cosine (hình 2.3 (b)). Do đó nhóm tác giả áp dụng phương pháp thống kê  $\chi^2$  với n bậc tự do cho các cặp PoV của các hệ số cosine ..., (-8, -7), (-6,-5), (-4, -3), (-2, -1), (2, 3), (4, 5), (6, 7)... không kiểm tra trên cặp (0, 1) vì cặp này ít sử dụng trong giấu tin [104].



Hình 2.3. Biểu đồ tần suất các hệ số cosine: a) ảnh gốc, b) ảnh có giấu tin [94]

Luận án thấy rằng phương pháp thống kê này cũng có thể áp dụng tương tự cho phát hiện ảnh có giấu tin trên miền tần số wavelet, vì nó cũng làm cân bằng các cặp PoV trên các hệ số wavelet.

Ngoài ra luận án đưa ra một phương pháp khác phát hiện mù cho ảnh có giấu tin trên LSB của các hệ số cosine cho kết quả tốt hơn trình bày trong mục sau.

### 2.2.2. Phương pháp phát hiện

Áp dụng biểu thức (2.11) được xây dựng từ mở rộng bổ đề Neyman – Pearson trong 2.1.3 cho miền tần số cosine ta có thuật toán dưới đây. Trong trường hợp không có ảnh gốc để so sánh chúng ta phải xây dựng một ảnh làm “mốc” bằng cách coi như ảnh được giấu tin với tỉ lệ giấu 100% tổng số các hệ số cosine có thể giấu của ảnh.

#### Thuật toán 2.6 – Thuật toán “Tỉ lệ xám 3”

**Đầu vào:** Cho tập ảnh  $\mathcal{V}$  (gồm có giấu tin trên LSB của hệ số cosine và ảnh gốc)

**Đầu ra:** Phân loại tập đó thành tập ảnh  $\mathcal{S}$  (có giấu trên LSB của hệ số cosine) và tập ảnh gốc  $\mathcal{C}$ .

*Các bước thực hiện*

**Bước 1:** Chọn lần lượt từng ảnh  $I$  trong tập ảnh  $\mathcal{V}$  biến đổi miền dữ liệu ảnh sang miền tần số cosine theo phép biến đổi cosine rời rạc [43]. Thực hiện bước 2 và 3 cho đến khi xét hết các ảnh trong  $\mathcal{V}$ .

**Bước 2:** Thống kê tần suất các hệ số cosine của ảnh I (bỏ qua các hệ số 0 và 1) vào vector  $X = \{x_i, i=1, 2, \dots, n\}$  (giá trị n được xác định từ số các hệ số có tần suất lớn hơn 0) với  $x_i$  là tần suất của hệ số cosine có giá trị i.

$$\text{Thực hiện tính } P_j^0 \text{ với } P_{2j}^0 = P_{2j+1}^0 = \frac{x_{2j} + x_{2j+1}}{2} \quad (0 < j < \frac{n}{2}).$$

$$\text{Áp dụng công thức (2.11) ta có: } T = \sum_{i=0}^n 2x_i \ln \frac{x_i}{(pq)P_i^0} \dots$$

**Bước 3:** Chọn ngưỡng  $t_0$ . Nếu  $T > t_0$  thì I lưu vào tập ảnh gốc  $\mathcal{C}$ , ngược lại I lưu vào tập ảnh  $\mathcal{S}$ .

Dựa vào tập thử nghiệm trên một tập ảnh lớn (1200 ảnh),  $t_0$  được chọn trong khoảng từ 200 đến 500.

Chúng ta có thể áp dụng thuật toán 2.6 cho miền tần số wavelet trên các băng tần cao LH, HL, HH bằng cách thay vì thống kê trên các hệ số cosine ta thống kê trên các hệ số wavelet.

## 2.3. CÁC KẾT QUẢ THỬ NGHIỆM

### 2.3.1. Các kết quả thử nghiệm trên miền không gian

#### 2.3.1.1. Thử nghiệm

*Tập ảnh thử nghiệm:* Sử dụng tập ảnh gốc  $\mathcal{C}_0$  gồm 2088 ảnh (nguồn gốc đã giới thiệu trong chương 1)

*Giấu tin trên LSB:* Tập ảnh  $\mathcal{C}_0$  được nhúng lượng thông tin trên miền LSB với tỉ lệ nhúng 30%, 50%, 70%, 100% bằng phương pháp giấu ngẫu nhiên (các điểm ảnh được chọn theo bộ chọn giả ngẫu nhiên PR) được bốn tập mới  $\mathcal{S}_{\text{LSB}_{30}}$ ,  $\mathcal{S}_{\text{LSB}_{50}}$ ,  $\mathcal{S}_{\text{LSB}_{70}}$ ,  $\mathcal{S}_{\text{LSB}_{100}}$  (mỗi tập 2088 ảnh).

*Phát hiện ảnh có giấu tin trên LSB:* Sử dụng các kỹ thuật phát hiện ảnh có giấu tin trên LSB của luận án (“độ lệch chuẩn”,  $\chi_1^2$ , “tỉ lệ xám 1”, “tỉ lệ xám 2”) và kỹ thuật phát hiện khác  $\chi_n^2$  [95] và LLRT [80] để phân loại ảnh có giấu tin và không giấu tin trên năm tập  $\mathcal{C}_0$ ,  $\mathcal{S}_{\text{LSB}_{30}}$ ,  $\mathcal{S}_{\text{LSB}_{50}}$ ,  $\mathcal{S}_{\text{LSB}_{70}}$ ,  $\mathcal{S}_{\text{LSB}_{100}}$ , ta được kết quả theo bảng 2.14 dưới đây.

**Bảng 2.14. Kết quả phân loại ảnh có giấu tin trên LSB trên các tập  $\mathcal{C}_0$ ,  $\mathcal{S}_{LSB_{30}}$ ,  $\mathcal{S}_{LSB_{50}}$ ,  $\mathcal{S}_{LSB_{70}}$ ,  $\mathcal{S}_{LSB_{100}}$  bằng một số kỹ thuật phát hiện ảnh có giấu tin**

| Tập ảnh<br>Kỹ thuật       | Tỉ lệ phân loại được trên từng tập ảnh (%) |              |           |              |                 |              |            |              |               |              |               |              |
|---------------------------|--|--------------|-----------|--------------|-----------------|--------------|------------|--------------|---------------|--------------|---------------|--------------|
|                           | $\chi_n^2$ [95]                            |              | LLRT [80] |              | “Độ lệch chuẩn” |              | $\chi_1^2$ |              | “Tỉ lệ xám 1” |              | “Tỉ lệ xám 2” |              |
|                           | Ảnh gốc                                    | Ảnh giấu tin | Ảnh gốc   | Ảnh giấu tin | Ảnh gốc         | Ảnh giấu tin | Ảnh gốc    | Ảnh giấu tin | Ảnh gốc       | Ảnh giấu tin | Ảnh gốc       | Ảnh giấu tin |
| $\mathcal{C}_0$           | 96.4                                       | 3.6          | 49.4      | 50.6         | 83.4            | 16.3         | 82.3       | 17.7         | 84.2          | 15.8         | 94.2          | 5.8          |
| $\mathcal{S}_{LSB_{30}}$  | 96.2                                       | 3.8          | 15.7      | 84.3         | 67.2            | 32.8         | 75.2       | 24.8         | 53.6          | 47.4         | 84.3          | 15.7         |
| $\mathcal{S}_{LSB_{50}}$  | 89.9                                       | 10.1         | 13.2      | 86.8         | 56.6            | 43.4         | 70.0       | 30.0         | 43.8          | 56.2         | 66.9          | 33.1         |
| $\mathcal{S}_{LSB_{70}}$  | 45.2                                       | 54.8         | 11.8      | 88.2         | 41.6            | 58.4         | 62.2       | 37.8         | 24.8          | 70.2         | 50.4          | 49.6         |
| $\mathcal{S}_{LSB_{100}}$ | 26.3                                       | 73.7         | 10.2      | 89.8         | 29.1            | 70.9         | 28.4       | 71.6         | 25.7          | 74.3         | 24.7          | 75.3         |

Đánh giá bằng độ đo  $P$ ,  $R$ ,  $F$ : Đánh giá kết quả trong bảng 2.14 theo độ đo  $P$  (Precision),  $R$  (Recall), độ trung bình điều hòa  $F$  trên tập ảnh  $\mathcal{W}$  gồm 10440 ảnh (gồm tập  $\mathcal{C}_0$ ,  $\mathcal{S}_{LSB_{30}}$ ,  $\mathcal{S}_{LSB_{50}}$ ,  $\mathcal{S}_{LSB_{70}}$ ,  $\mathcal{S}_{LSB_{100}}$ ) ta được kết quả trong bảng 2.15.

**Bảng 2.15. Kết quả đánh giá bằng các độ đo  $P$ ,  $R$ ,  $F$  trên tập ảnh  $\mathcal{W}$  gồm 10440 ảnh ( $\mathcal{C}_0$  và  $\mathcal{S}_{LSB_{30}}$ ,  $\mathcal{S}_{LSB_{50}}$ ,  $\mathcal{S}_{LSB_{70}}$ ,  $\mathcal{S}_{LSB_{100}}$ )**

| Kỹ thuật \ Độ đo | P    | R    | F    |
|------------------|------|------|------|
| $\chi_n^2$ [95]  | 0.36 | 0.98 | 0.52 |
| LLRT [80]        | 0.87 | 0.87 | 0.87 |
| “Độ lệch chuẩn”  | 0.51 | 0.92 | 0.66 |
| $\chi_1^2$       | 0.41 | 0.90 | 0.56 |
| “Tỉ lệ xám 1”    | 0.62 | 0.94 | 0.75 |
| “Tỉ lệ xám 2”    | 0.43 | 0.96 | 0.59 |

Từ bảng 2.15 cho thấy xét trên các trường hợp giấu tin với các tỉ lệ giấu khác nhau thì giá trị của  $F$  là nhỏ (0.52 – 0.87), trong đó  $\chi_n^2$  cho kết quả thấp nhất vì kỹ thuật này chỉ phát hiện tốt cho tập ảnh gốc và tập ảnh có giấu tin với tỉ lệ bit giấu cao nhất, còn kỹ thuật LLRT cho giá trị  $F$  cao nhất vì khi ảnh chỉ cần giấu một tỉ lệ nhỏ nó đã kết luận là ảnh có giấu tin do phương pháp xây dựng ảnh gốc là “trơn” như đã phân tích trong chương 1, các kỹ thuật đề xuất của luận án cho kết quả

tương đương nhau. Điều này cho thấy với tỉ lệ giấu thấp các kỹ thuật phát hiện mù cho kết quả phân loại không cao.

Đánh giá độ đo P, R, F trên tập ảnh  $\mathcal{O}$  gồm 4176 ảnh (tập  $\mathcal{C}_0, \mathcal{S}_{LSB_{100}}$ ) là tập gồm các ảnh gốc và ảnh được giấu với tỉ lệ bit giấu lớn nhất (100%) trên miền LSB cho các kỹ thuật phân loại mù trên cho ảnh có giấu trên LSB ta được kết quả trong bảng 2.16.

**Bảng 2.16. Kết quả đánh giá bằng các độ đo P, R, F trên tập ảnh  $\mathcal{O}$  gồm 4176 ảnh (tập  $\mathcal{C}_0, \mathcal{S}_{LSB_{100}}$ )**

| Kỹ thuật \ Độ đo | P    | R    | F    |
|------------------|------|------|------|
| $\chi_n^2$ [95]  | 0.74 | 0.95 | 0.83 |
| LLRT [80]        | 0.89 | 0.64 | 0.74 |
| “Độ lệch chuẩn”  | 0.71 | 0.81 | 0.75 |
| $\chi_1^2$       | 0.72 | 0.80 | 0.76 |
| “Tỉ lệ xám 1”    | 0.74 | 0.82 | 0.78 |
| “Tỉ lệ xám 2”    | 0.75 | 0.92 | 0.82 |

Từ bảng 2.16 cho thấy kết quả giá trị của P, R, F của các kỹ thuật phát hiện là rất cao cho trường hợp phân loại ảnh gốc và ảnh có giấu với tỉ lệ giấu lớn nhất cho phép của ảnh (100%), trong đó kỹ thuật LLRT [80] có giá trị F là nhỏ nhất, “tỉ lệ xám 2” và “ $\chi_n^2$ ” cho kết quả tốt nhất.

*Ước lượng thông tin:* Sử dụng ba kỹ thuật ước lượng tỉ lệ thông tin giấu trên miền LSB: kỹ thuật RS [31], DI [102], “trùng khớp” (luận án đề xuất) trên năm tập  $\mathcal{C}_0, \mathcal{S}_{LSB_{30}}, \mathcal{S}_{LSB_{50}}, \mathcal{S}_{LSB_{70}}, \mathcal{S}_{LSB_{100}}$ , ta được kết quả theo bảng 2.17, trong đó chúng ta tính giá trị trung bình  $\bar{x}$  theo (1.8) ước lượng được trên mỗi tập ảnh và độ lệch  $s$  theo (1.7) trên tập ước lượng tính.



**Bảng 2.17. Kết quả ước lượng trên năm tập  $C_0, S_{LSB_{30}}, S_{LSB_{50}}, S_{LSB_{70}}, S_{LSB_{100}}$**

| Kỹ thuật<br>Tập ảnh | RS        |       | DI        |       | “Trùng khớp” |       |
|---------------------|-----------|-------|-----------|-------|--------------|-------|
|                     | $\bar{x}$ | $S$   | $\bar{x}$ | $s$   | $\bar{x}$    | $s$   |
| $C_0$               | 0.04      | 0.816 | 0.73      | 26.3  | 3.15         | 20.36 |
| $S_{LSB_{30}}$      | 22.17     | 1.36  | 37.22     | 12.53 | 36.25        | 33.48 |
| $S_{LSB_{50}}$      | 63.4      | 15.1  | 51.43     | 40.37 | 52.17        | 40.15 |
| $S_{LSB_{70}}$      | 83.2      | 19.7  | 76.82     | 11.50 | 81.7         | 31.5  |
| $S_{LSB_{100}}$     | 96.3      | 15.7  | 98.23     | 9.02  | 93.87        | 12.8  |

*So sánh thời gian thực hiện:* Thực hiện kiểm tra thời gian thực hiện các kỹ thuật phát hiện và kỹ thuật ước lượng thông tin trên cùng một tập ảnh  $C_0$  (2088 ảnh) ta được kết quả theo bảng 2.18.

**Bảng 2.18. Kết quả thời gian thực hiện phân loại trên tập  $C_0$  (2088 ảnh)**

| Kỹ thuật         | $\chi_n^2$ | LLRT | Độ lệch chuẩn | $\chi_1^2$ | Tỉ lệ xám 1 | Tỉ lệ xám 2 | RS   | DI   | “Trùng khớp” |
|------------------|------------|------|---------------|------------|-------------|-------------|------|------|--------------|
| Thời gian (giây) | 156        | 73   | 153           | 153        | 52          | 83          | 6821 | 2236 | 185          |

Bảng 2.17, 2.18 cho thấy kỹ thuật phát hiện “Trùng khớp” cho kết quả ước lượng tương đương RS [31] và DI [102]. Tuy nhiên kỹ thuật ước lượng “Trùng khớp” cho thời gian thực hiện nhanh hơn hai kỹ thuật ước lượng RS và DI theo phân tích số phép tính phải thực hiện của từng thuật toán ứng với từng kỹ thuật ước lượng dưới đây.

- Số phép tính sử dụng trong thuật toán “trùng khớp” bao gồm: hai vòng lặp lồng nhau để thống kê các tần suất điểm ảnh của ảnh, và một vòng lặp để xây dựng ảnh làm “mốc” giấu xấp xỉ 100% thông tin trên LSB, sau đó sử dụng một vòng lặp đơn để tính độ lệch giữa các cặp giá trị của miền không

gian ảnh kiểm tra và miền không gian ảnh sau khi ước lượng. Ngoài ra phải tính toán một số biểu thức ước lượng.

- Số phép tính sử dụng của RS bao gồm: ba vòng lặp lồng nhau, trong đó hai vòng lặp ngoài dùng để chia miền không gian ảnh thành các miền không gian nhỏ hơn, mỗi miền con lại phải thực hiện một vòng lặp đơn để kiểm tra miền này là miền đều đặn (R), miền dị thường (S), hay miền không sử dụng (U), thêm một số phép tính để ước lượng thông tin từ miền R và miền S. Vì vậy có thể thấy số phép tính thực hiện lớn hơn “Trùng khớp”.
- Số phép tính sử dụng của DI bao gồm bốn lần vòng lặp đôi lồng nhau: một vòng lặp đôi để tính giá trị sai phân của các điểm ảnh; một vòng lặp đôi để đảo các bit LSB của ảnh đầu vào được một miền không gian mới và tính giá trị sai phân của miền không gian mới này; một vòng lặp đôi để chuyển các bit LSB có giá trị 1 thành 0 tạo ra một miền không gian mới và tính giá trị sai phân của nó; một vòng lặp đôi để thống kê các tần suất sai phân của ba miền không gian trên, trong vòng lặp đôi này sử dụng thêm một vòng lặp đơn để lưu giá trị thống kê vào một vector một chiều. Ngoài ra một số phép tính đơn khác. Vì vậy có thể thấy số phép tính thực hiện lớn hơn “Trùng khớp”.

Do đó thuật toán của kỹ thuật “Trùng khớp” cho thời gian thực hiện nhanh hơn kỹ thuật RS và DI, theo bảng 2.18 thời gian thực hiện của “trùng khớp” trên một tập 2088 ảnh là 185 (giây) chỉ bằng 1/37 lần kỹ thuật RS và bằng 1/12 lần kỹ thuật ước lượng DI.

### **2.3.1.2. Nhận xét**

Từ kết quả thử nghiệm và đánh giá trong các bảng 2.14 – 2.18 luận án đưa ra một số nhận xét sau:

- Kỹ thuật “độ lệch chuẩn” *không tốt hơn* kỹ thuật “ $\chi_n^2$ ” ở trường hợp phân loại ảnh tập ảnh gốc nhưng *tốt hơn* trong trường hợp phân loại ảnh có giấu tin, vì kỹ thuật “ $\chi_n^2$ ” chỉ tốt khi thông tin được giấu một cách tuần tự (theo chiều quét raster) trên miền LSB của ảnh.

- Kỹ thuật “LLRT” của Sullivan rất tốt trong trường hợp phân loại ảnh có giấu tin, nhưng không tốt trong trường hợp phân loại ảnh gốc vì tác giả sử dụng lọc thông thấp để xây dựng xấp xỉ ảnh gốc từ vector tần suất của một ảnh bất kỳ, kết quả lọc thông thấp thường cho tín hiệu ảnh “trơn” hơn một ảnh gốc tự nhiên (như đã minh họa trong chương 1, hình 1.4), vì vậy nó làm cho phát hiện sai lệch ảnh gốc thực tế (bảng 2.14).
- “Tỉ lệ xám 2” và “ $\chi_n^2$ ” cho kết quả phân loại tương đương trong tập ảnh có giấu tin và không giấu tin.
- Theo đánh giá P, R, F trong các bảng 2.15 và 2.16 thì giá trị của P, R, F chỉ cao khi phân loại tập ảnh gốc và ảnh có giấu tin với tỉ lệ giấu thông tin lớn nhất (100% trên LSB). Còn cho tất cả các trường hợp thì độ tin cậy chỉ xấp xỉ bằng 0.56.
- Thời gian phân loại trên cùng tập ảnh của kỹ thuật “tỉ lệ xám 1” và “tỉ lệ xám 2” xấp xỉ kỹ thuật “LLRT” vì số phép tính trong các kỹ thuật này xấp xỉ nhau vì đều cùng sử dụng các phép tính logarit trong tính toán.
- Phương pháp phát hiện bằng ước lượng “Trùng khớp” có thể ước lượng tương đương RS và DI nhưng thời gian thực hiện của “Trùng khớp” nhanh hơn cả (bảng 2.18).

### 2.3.2. Các kết quả thử nghiệm trên miền tần số

#### 2.3.2.1. Thử nghiệm

*Tập ảnh thử nghiệm:* là tập ảnh  $J_0$  gồm 1200 ảnh JPEG trong đó 605 ảnh chụp từ máy ảnh kỹ thuật số, và 595 ảnh tải về từ [103, 107].

*Giấu thông tin:* Tập ảnh  $J_0$  được giấu lượng thông tin với tỉ lệ bit giấu 25%, 50% và 100% trên miền hệ số cosine của các ảnh được các tập ảnh  $J_{25}$ ,  $J_{50}$ ,  $J_{100}$  có giấu tin trên LSB của các hệ số cosine.

Phát hiện ảnh có giấu tin: Sử dụng thuật toán 2.6 (tỉ lệ xám 3) và thuật toán của kỹ thuật  $\chi_n^2$  [95] để phân loại ảnh cho các tập ảnh  $J_0, J_{25}, J_{50}, J_{100}$  ta được kết quả phân loại trong bảng 2.19.

**Bảng 2.19: Tỉ lệ phân loại ảnh của kỹ thuật “tỉ lệ xám 3” và  $\chi_n^2$  [71] với các tập ảnh  $J_0, J_{25}, J_{50}, J_{100}$**

| Tập dữ liệu ảnh | $\chi_n^2$ [95] |                  | “Tỉ lệ xám 3” |                  |
|-----------------|-----------------|------------------|---------------|------------------|
|                 | Ảnh gốc (%)     | Ảnh giấu tin (%) | Ảnh gốc (%)   | Ảnh giấu tin (%) |
| $J_0$           | 93.7            | 6.3              | 91.8          | 8.2              |
| $J_{25}$        | 83.5            | 16.5             | 75.6          | 24.4             |
| $J_{50}$        | 48.7            | 51.3             | 42.3          | 57.7             |
| $J_{100}$       | 10.4            | 89.6             | 3.9           | 96.1             |

Đánh giá kết quả trong bảng 2.19 theo độ đo P (Precision), R (Recall), độ trung bình điều hòa trên tập ảnh  $J$  gồm 4800 ảnh (gồm tập  $J_0, J_{25}, J_{50}, J_{100}$ ) ta được kết quả trong bảng 2.20.

**Bảng 2.20. Kết quả đánh giá bằng các độ đo P, R, F trên tập ảnh  $J$**

| Độ đo               | P    | R    | F    |
|---------------------|------|------|------|
| Kỹ thuật $\chi_n^2$ | 0.52 | 0.96 | 0.68 |
| “tỉ lệ xám 3”       | 0.59 | 0.95 | 0.73 |

Bảng 2.21 là thời gian thực hiện trên tập  $J_0$  gồm 1200 ảnh của hai kỹ thuật phát hiện  $\chi_n^2$  và “tỉ lệ xám 3”.

**Bảng 2.21. Thời gian thực hiện trên tập  $J_0$**

| Kỹ thuật phát hiện         | $\chi_n^2$ | “Tỉ lệ xám 3” |
|----------------------------|------------|---------------|
| Thời gian thực hiện (giây) | 488        | 166           |

### **2.3.2.2. Nhận xét**

Phát hiện ảnh có giấu tin trên miền tần số: Kỹ thuật “tỉ lệ xám 3” phát hiện ảnh có giấu tin trên LSB của các hệ số cosine phân loại xấp xỉ kỹ thuật “ $\chi_n^2$ ” cho trường hợp ảnh gốc nhưng tốt hơn cho trường hợp ảnh giấu tin với tỉ lệ 100% miền hệ số cosine, và thời gian thực hiện của “tỉ lệ xám 3” cũng nhanh hơn “ $\chi_n^2$ ” (gần 3 lần).

## **KẾT LUẬN CHƯƠNG 2**

Chương này đưa ra bốn phương pháp cải tiến phát hiện mù cho ảnh có giấu tin trên LSB của miền không gian và một phương pháp phát hiện mù trên LSB của miền tần số. Dựa trên tập thử nghiệm gồm 2088 ảnh để so sánh kỹ thuật cải tiến của luận án với một số kỹ thuật phát hiện mù khác.

Các kết quả thử nghiệm cho thấy các kỹ thuật phát hiện do luận án đưa ra trong chương này là tương đương hoặc tốt hơn kỹ thuật phát hiện khác trong một số trường hợp ảnh có tỉ lệ bit giấu thấp hoặc thời gian thực hiện.

### **Chương 3. MỘT SỐ KỸ THUẬT PHÁT HIỆN CÓ RÀNG BUỘC**

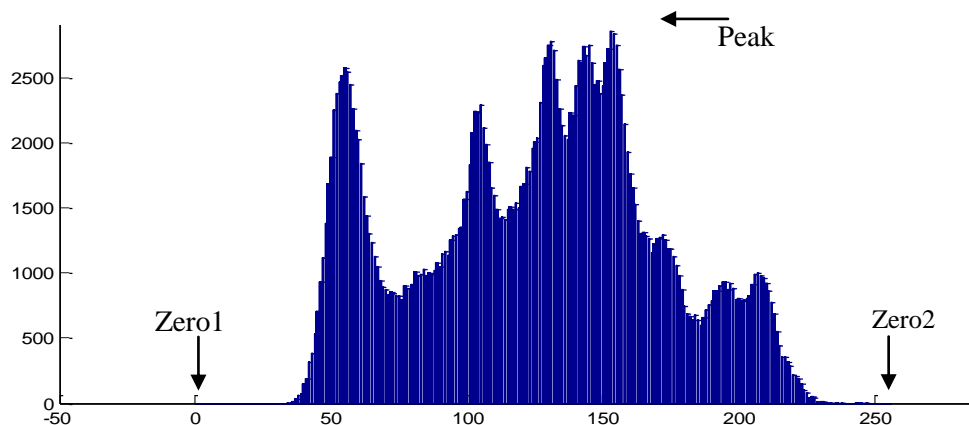
Chương này đưa ra bốn kỹ thuật phát hiện có ràng buộc cho ảnh có giấu tin sử dụng kỹ thuật giấu tin DIH, IWH, HKC, RVH. Chúng đều là trường hợp riêng của kỹ thuật giấu LSB, tuy nhiên tỉ lệ thay đổi trên LSB của ảnh thường thấp so với lượng thông tin đem giấu (hoặc kích cỡ ảnh), vì vậy phát hiện bằng các kỹ thuật phát hiện mù trên LSB của ảnh thường cho kết quả không cao. Trong phần này luận án đưa ra các phương pháp phát hiện tối ưu hơn so với phát hiện mù trên LSB cho các kỹ thuật giấu DIH, IWH, HKC, RVH và phương pháp ước lượng xấp xỉ lượng bit thông tin giấu trong ảnh sử dụng các kỹ thuật này.

#### **3.1. PHÁT HIỆN ẢNH CÓ GIẤU TIN SỬ DỤNG KỸ THUẬT GIẤU HKC**

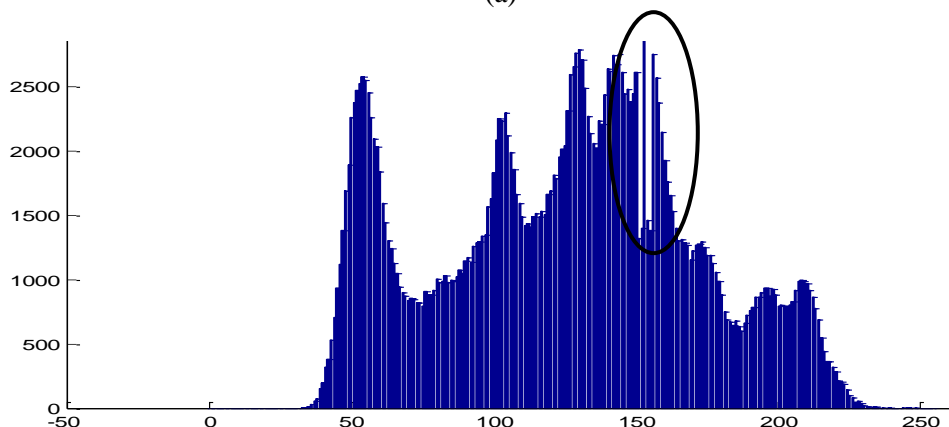
##### **3.1.1. Tóm lược kỹ thuật giấu HKC**

Kỹ thuật HKC do J. H. Hwang, J.W. Kim và J. U. Choi đề xuất năm 2006 [41], dựa trên phương pháp dịch chuyển biểu đồ tần suất như sau: chọn điểm có tần suất lớn nhất (gọi là điểm Peak) trong biểu đồ, sau đó chọn hai điểm Zero1 và Zero2 (các điểm có cột tần suất có giá trị bằng 0) ở bên trái và bên phải điểm Peak (ví dụ hình 3.1 (a) biểu đồ tần suất của ảnh 8-bit Lena.bmp). Sau đó thực hiện làm rộng hai cột tần suất tại vị trí Peak+1 và Peak -1. Để có thể khôi phục ảnh gốc, bản đồ định vị được đề xuất dùng để lưu trữ thông tin vị trí của các điểm gồm: điểm Peak, Zero1, giá trị tần suất Zero1, điểm Zero2, tần suất của điểm Zero2. Bản đồ định vị này chuyển thành một chuỗi nhị phân và được ghép vào trước chuỗi thông tin M cùng giấu vào ảnh.

Thực hiện giấu thông tin vào ảnh theo nguyên tắc: giả sử cần giấu bit  $b$ , quét ảnh (theo thứ tự từ trái sang phải từ trên xuống) nếu điểm ảnh có giá trị bằng Peak - 2 hoặc Peak + 2, thì kiểm tra bit  $b$  cần nhúng trong chuỗi bit thông tin: nếu bit thông tin là “1” thì điểm ảnh có giá trị là Peak - 2 sẽ tăng lên 1, hoặc điểm ảnh có giá trị là Peak + 2 sẽ giảm đi 1, còn nếu bit thông tin là “0” thì vẫn duy trì như cũ (ngầm hiểu đã giấu vào Peak -2 hoặc Peak +2). Kết thúc quá trình giấu tin ta được ảnh stego có giấu tin với biểu đồ tần suất trong hình 3.1 (b)



(a)



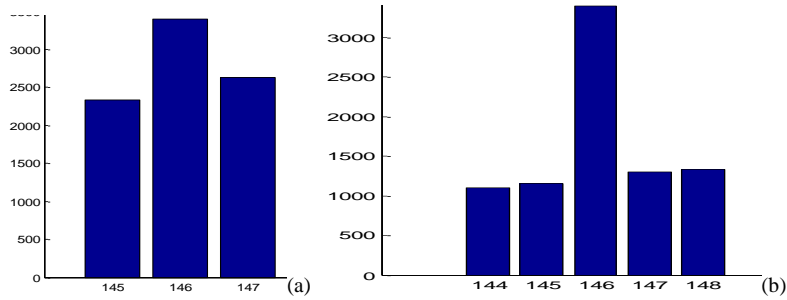
(b)

Hình 3.1. Biểu đồ tần suất: (a) ảnh gốc, (b) ảnh giấu tin bằng HKC

### 3.1.2. Phương pháp phát hiện và ước lượng thông tin giấu trong ảnh

#### 3.1.2.1. Phương pháp phát hiện của Kuo và Lin

Năm 2008, Wen – Chung Kuo (Kuo) và Yan – Hung Lin (Lin) đề xuất kỹ thuật phát hiện ảnh giấu tin sử dụng HKC [46]. Họ quan sát biểu đồ tần suất 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 3.2 (a) và (b), vì vậy họ đưa ra định lý 3.1 để xây dựng kỹ thuật phát hiện dưới đây.



Hình 3.2. Điểm Peak: (a) trước khi giấu tin, (b) sau khi giấu tin

**Định lý 3.1** - Có năm 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 năm điểm liên tục và mối quan hệ láng giềng được xác định lần lượt như biểu thức (3.1) và (3.2):

$$\frac{y_3 - y_2}{y_3} \approx \frac{y_3 - y_4}{y_3} \approx \tau_1, 0.4 \leq \tau_1 \leq 0.6 \quad (3.1)$$

$$\left| \frac{y_1 - y_2}{y_2} \right| \approx \left| \frac{y_4 - y_5}{y_4} \right| \leq \tau_2 \quad (3.2)$$

$\tau_2$  là giá trị ngưỡng

Trong [46], tác giả lấy  $\tau_2 = 0.1$ .

Áp dụng định lý này, Kuo và Lin đưa ra thuật toán phát hiện ảnh có giấu tin sử dụng kỹ thuật HKC sau đây:

### **Thuật toán 3.1 – Phát hiện ảnh stego\_HKC của Kuo và Lin**

**Đầu vào:** Một ảnh 8 – bit cấp độ màu C

**Đầu ra:** kiểm tra xem C có giấu tin sử dụng kỹ thuật giấu HKC hay không

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

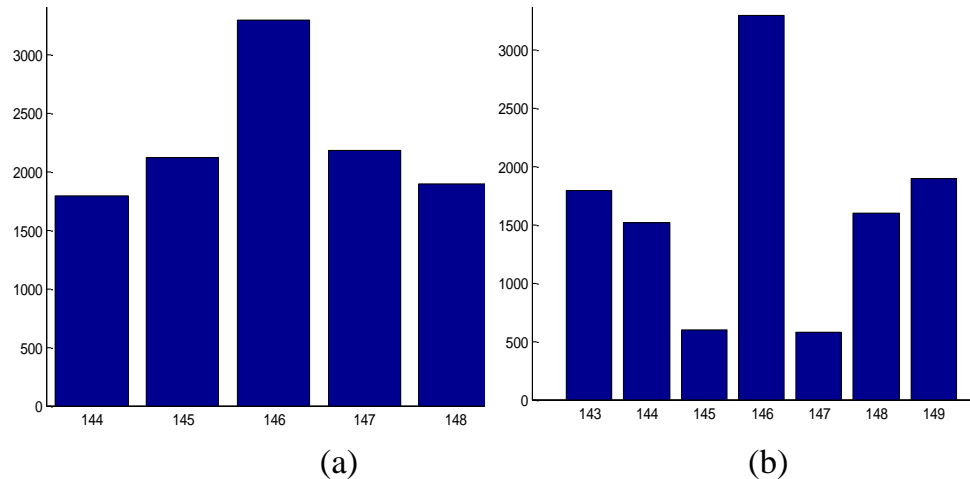
**Bước 2.** Tính tỷ lệ thay đổi và mối quan hệ láng giềng với  $(x_{\max}, y_{\max})$  sử dụng định lý 3.1.

**Bước 3.** Nếu năm cặp giá trị liên tiếp lân cận  $(x_{\max}, y_{\max})$  thỏa mãn (3.1) và (3.2), thì kết luận ảnh C có giấu tin vùng điểm Peak, ngược lại ảnh không giấu tin.



### 3.1.2.2. Phương pháp phát hiện cải tiến từ phương pháp của Kuo và Lin

Với kỹ thuật phát hiện của Kuo và Lin (dựa trên định lý 3.1) trong một số trường hợp, chúng ta thấy nó không phù hợp khi thông tin không được giấu hết vào vị trí của cột tần suất có giá trị lân cận điểm Peak.



Hình 3.3. Biểu đồ tần suất của: (a) ảnh gốc, (b) ảnh giấu tin bằng HKC

Ví dụ như hình 3.3 (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 tần suất của 2 điểm này, nên tần suất có giá trị điểm ảnh bằng 144 không bằng tần suất có giá trị điểm ảnh là 145 và tần suất có giá trị điểm ảnh là 147 không bằng tần suất có giá trị điểm ảnh là 148 (xem hình 3.3 (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 (3.1) và (3.2) ta thấy:

$$(y_3 - y_2) / y_3 = 0.8182 \text{ và } (y_3 - y_4) / y_3 = 0.8242 \text{ và}$$

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

không thỏa mãn định lý 3.1.

Để cải tiến kỹ thuật của Kuo và Lin phát hiện hiệu quả hơn cho trường hợp giấu với lượng giấu khác nhau, ta có định lý 3.2 như sau:

*Định lý 3.2 - Có năm 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 (với điểm ảnh có giá trị  $x_3$  có tần suất lớn nhất  $y_3$ ). Khi đó ảnh có giấu tin sử dụng kỹ thuật giấu HKC nếu mối quan hệ của năm cặp giá trị này thỏa mãn biểu thức (3.1') và (3.2'):*

$$\frac{y_3 - y_2}{y_3} \approx \frac{y_3 - y_4}{y_3} \approx \tau_1, 0.4 \leq \tau_1 < 1 \quad (3.1')$$

$$\frac{y_2}{y_1} \approx \frac{y_4}{y_5} \leq 1 \quad (3.2')$$

Chứng minh:

Giả thiết  $(x_3, y_3)$  là cặp giá trị với điểm ảnh có giá trị  $x_3$  có tần suất  $y_3$  là lớn nhất. Các giá trị  $x_1, x_2$  là các giá trị lân cận trái của  $x_3$  và  $x_4, x_5$  là các giá trị lân cận phải của  $x_3$ .

Theo giả thuyết của kỹ thuật giấu tin HKC giá trị tần suất của  $x_2$  (là  $y_2$ ) và  $x_4$  (là  $y_4$ ) có giá trị gần xấp xỉ bằng  $y_3$ , do đó có thể giấu tin được nhiều thông tin vào các lân cận này, nên ta có mối quan hệ sau trong các ảnh chưa giấu tin bằng HKC:

$$y_2 \approx y_3, y_4 \approx y_3$$

$$\text{Hay: } \frac{y_3 - y_2}{y_3} \approx \frac{y_3 - y_4}{y_3} < 0.4 \quad (3.3)$$

Để có thể giấu tin, HKC thực hiện biến đổi các cột tần số tại  $y_1, y_2, y_4, y_5$  như sau:

$$y'_1 = y_2, y'_2 = 0, y'_5 = y_4, y'_4 = 0 \quad (\text{tạo thành cột tần suất rỗng tại } y'_2 \text{ và } y'_4).$$

Giả sử ta cần giấu một chuỗi bit thông tin  $M$  có độ dài  $m$ .

Theo kỹ thuật giấu HKC thì sẽ thay đổi một phần tần suất gần bằng  $m/4$  trong  $y'_1$  thành  $y'_2$ , và  $m/4$  giá trị tần suất của  $y'_5$  thành  $y'_4$ . Lượng bit còn lại ( $2 * m/4$ ) ngầm định giấu trong  $y'_1$  và  $y'_5$ . Nghĩa là lượng bit giấu trong ảnh  $m = 2 * (y'_2 + y'_4)$ , vì chuỗi thông tin giấu là đại lượng ngẫu nhiên có phân bố i.i.d [61] nên xác suất bit "0" và xác suất bit "1" xấp xỉ bằng nhau và bằng 0.5 ( $P(0) \approx P(1) = 0.5$ )

+ Trường hợp giấu số bit hết khả năng của ảnh thì:

$$y'_1 \approx y'_2 \approx y_2/2$$

$$y'_4 \approx y'_5 \approx y_4/2$$

$$m = y'_1 + y'_2 + y'_4 + y'_5 = 2 * (y'_1 + y'_5)$$

$$\text{Do đó } \frac{y_3 - y_2'}{y_3} \approx \frac{y_3 - y_4'}{y_3} > 0.4 \quad (3.4)$$

+ Trường hợp giấu với lượng giấu rất nhỏ nghĩa là  $y_2'$  và  $y_4'$  rất nhỏ gần tới 0 thì

$$\frac{y_3 - y_2'}{y_3} \approx \frac{y_3 - y_4'}{y_3} < 1 \quad (3.5)$$

Tuy nhiên trong một số trường hợp (II) có thể thỏa mãn với ảnh không giấu tin hoặc các cột tần suất lân cận trái hoặc phải của  $y_3$  có giá trị gần bằng 1/2 giá trị của  $y_3$  do đó ta hạn chế bằng biểu thức sau:

Sau khi giấu tin:

$$+ y_2' \approx y_4'$$

$$+ y_2' \leq y_1'$$

$$+ y_4' \leq y_5'$$

Do đó ta có :

$$\frac{y_2'}{y_1'} \approx \frac{y_4'}{y_5'} \leq 1 \quad (3.6)$$

Từ (3.3), (3.4), (3.5), (3.6) ta có điều phải chứng minh.

Áp dụng định lý này vào bài toán phát hiện ảnh giấu sử dụng HKC ta được thuật toán 3.2 như sau:

### **Thuật toán 3.2 – Phát hiện ảnh stego\_HKC\_cải tiến**

**Đầu vào:** Một ảnh 8 – bit cấp độ màu C

**Đầu ra:** Kiểm tra xem ảnh C có giấu tin sử dụng kỹ thuật giấu HKC hay không

**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 với ( $x_{\max}$ ,  $y_{\max}$ ) sử dụng định lý 3.2.

**Bước 3.** Nếu năm cặp giá trị liên tiếp lân cận ( $x_{\max}$ ,  $y_{\max}$ ) thỏa mãn (3.1') và (3.2'), thì kết luận ảnh C có giấu tin trong vùng này, ngược lại ảnh không giấu tin.

Sau khi thử nghiệm và khảo sát lại trên một tập ảnh lớn chúng ta có thể đưa một biểu thức kiểm tra khác đơn giản và tối ưu hơn kỹ thuật cải tiến của Kuo và

Lin. Từ biểu thức mới này chúng ta còn có thể ước lượng được lượng bit thông tin đã giấu trong ảnh bằng HKC trong khi kỹ thuật của Kuo và Lin chưa đưa ra. Chi tiết được trình bày trong 3.1.2.3 dưới đây

### 3.1.2.3. Phương pháp phát hiện HKC khác và ước lượng thông tin giấu

Gọi  $\{h_i\}_{i=0}^{255}$  là vector tần suất của ảnh gốc trước khi giấu tin, khi đó Peak là điểm ảnh có tần suất ( $h_{\text{Peak}}$ ) lớn nhất, các cột tần suất lân cận  $h_{\text{Peak}-2}$ ,  $h_{\text{Peak}-1}$ ,  $h_{\text{Peak}+1}$ ,  $h_{\text{Peak}+2}$  có giá trị lớn xấp xỉ  $h_{\text{Peak}}$ , vì vậy tổng tần suất của  $h_{\text{Peak}+1}$  và  $h_{\text{Peak}+2}$  (hoặc  $h_{\text{Peak}-1}$  và  $h_{\text{Peak}-2}$ ) sẽ luôn lớn hơn  $h_{\text{Peak}}$ , nghĩa là  $h_{\text{Peak}+1} + h_{\text{Peak}+2} > h_{\text{Peak}}$  (hoặc  $h_{\text{Peak}-1} + h_{\text{Peak}-2} > h_{\text{Peak}}$ ) điều này có thể nhìn trực quan theo hình 3.1. (a)

Với ảnh có giấu tin thì điều này lại ngược lại, vì để giấu tin theo HKC chúng ta phải dịch chuyển tần suất  $h_{\text{Peak}+2}$  sang vị trí  $h_{\text{Peak}+3}$ ,  $h_{\text{Peak}+1}$  sang  $h_{\text{Peak}+2}$ ,  $h_{\text{Peak}-2}$  sang  $h_{\text{Peak}-3}$ ,  $h_{\text{Peak}-1}$  sang  $h_{\text{Peak}-2}$ . Khi thông tin được giấu vào ảnh sẽ dịch chuyển một phần  $h_{\text{Peak}-2}$  sang  $h_{\text{Peak}-1}$  và  $h_{\text{Peak}+2}$  sang  $h_{\text{Peak}+1}$ . Do đó chúng ta thấy  $h_{\text{Peak}-1} + h_{\text{Peak}-2} < h_{\text{Peak}}$  và  $h_{\text{Peak}+1} + h_{\text{Peak}+2} < h_{\text{Peak}}$  vì  $h_{\text{Peak}-1} + h_{\text{Peak}-2}$  và  $h_{\text{Peak}+1} + h_{\text{Peak}+2}$  chính là tần suất của  $h_{\text{Peak}-1}$  và  $h_{\text{Peak}+1}$  trong ảnh gốc ban đầu (có thể trực quan theo hình 3.1. (b)).

Cũng dựa vào mối quan hệ bị thay đổi này giữa các vùng lân cận  $h_{\text{Peak}}$  chúng ta có thể ước lượng được số bit thông tin giấu trong ảnh dựa vào  $h_{\text{Peak}-1}$  và  $h_{\text{Peak}+1}$ . Ban đầu để giấu tin chúng ta phải dịch chuyển  $h_{\text{Peak}-1}$  sang  $h_{\text{Peak}-2}$ ,  $h_{\text{Peak}+1}$  sang  $h_{\text{Peak}+2}$ , nghĩa là làm cho  $h_{\text{Peak}-1} = 0$ ,  $h_{\text{Peak}+1} = 0$ . Sau khi giấu tin các bit “1” của chuỗi thông tin làm dịch chuyển một phần  $h_{\text{Peak}-2}$ ,  $h_{\text{Peak}+2}$  sang  $h_{\text{Peak}-1}$ ,  $h_{\text{Peak}+1}$  (theo thuật toán giấu HKC) còn các bit “0” ngầm định được giấu vào các điểm ảnh Peak-2 và Peak+2.

Gọi  $L_0$ ,  $L_1$  là số bit “0” và bit “1” của chuỗi thông tin M cần giấu khi đó:  $L_1 = h_{\text{Peak}-1} + h_{\text{Peak}+1}$ , còn  $L_0 \approx L_1$  vì chuỗi thông tin M là đại lượng ngẫu nhiên có phân bố i.i.d [61] nên xác suất bit “0” và xác suất bit “1” xấp xỉ bằng nhau và bằng 0.5 ( $P(0) \approx P(1) = 0.5$ ). Vậy độ dài bit thông tin M được giấu trong ảnh sử dụng HKC được tính theo biểu thức sau:  $L = 2L_1 = 2(h_{\text{Peak}-1} + h_{\text{Peak}+1})$ .

Từ các vấn đề phân tích ở trên chúng tôi có được định lý 3.3 cho phát hiện ảnh có giấu tin sử dụng kỹ thuật giấu HKC.

*Định lý 3.3 - Có năm 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  $x_3$  và  $y_3 = h_{Peak}$ . Khi đó ảnh có giấu tin bằng HKC nếu mỗi quan hệ của năm điểm này thỏa mãn:*

$$y_1 + y_2 < y_3 \quad (3.7)$$

$$y_4 + y_5 < y_3 \quad (3.8)$$

và lượng bit thông tin đã giấu được tính bằng biểu thức:

$$L = 2(y_2 + y_4) \quad (3.9)$$

Chứng minh:

Theo giả thuyết cặp giá trị  $(x_3, y_3)$  là cặp giá trị với điểm Peak là  $x_3$  có tần suất  $y_3$  là lớn nhất. Các giá trị  $x_1, x_2$  là các giá trị lân cận  $x_3$  về bên trái,  $x_4, x_5$  là các giá trị lân cận về bên phải. Vì vậy các giá trị này có  $y_1, y_2, y_4, y_5$  tương ứng lớn gần bằng  $y_3$  nên có mối quan hệ:

$$y_1 < y_3, y_2 < y_3, y_4 < y_3, y_5 < y_3 \quad (3.10)$$

$$y_1 + y_2 > y_3$$

$$y_4 + y_5 > y_3$$

Trước khi giấu tin, HKC thực hiện biến đổi các cột tần số tại  $y_1, y_2, y_4, y_5$  như sau:

$$y'_1 = y_2, y'_2 = 0, y'_5 = y_4, y'_4 = 0$$

nghĩa là  $y_2$  bị dịch chuyển thành  $y_1$ ,  $y_4$  bị dịch chuyển thành  $y_5$  (tức là tạo thành cột tần suất rỗng tại  $y_2$  và  $y_4$ ).

Sau khi giấu tin một phần tần suất trong  $y'_1$  chuyển sang  $y'_2$ ,  $y'_5$  chuyển sang  $y'_4$ .

Mà  $y'_1 + y'_2 = y_2$ ,  $y'_4 + y'_5 = y_4$  theo (3.10) chúng ta có  $y_2 < y_3$ ,  $y_4 < y_3$ . Nghĩa là sau khi giấu tin:

$$y'_1 + y'_2 < y_3, y'_4 + y'_5 < y_3 \quad (3.11)$$

Nếu (3.11) thỏa mãn thì ta có thể tính được lượng bit thông tin giấu xấp xỉ trong ảnh bằng HKC như sau:

Gọi  $L_0, L_1$  là số bit "0" và bit "1" của chuỗi thông tin  $M$  cần giấu khi đó:  $L_1 = y'_2 + y'_4$ , mặt khác  $L_0 \approx L_1$  vì chuỗi thông tin  $M$  là đại lượng ngẫu nhiên có phân bố i.i.d [61] nên xác suất bit "0" và xác suất bit "1" xấp xỉ bằng nhau và bằng 0.5 ( $P(0)$

$\approx P(1) = 0.5$ ). Vậy độ dài bit thông tin  $M$  được giấu trong ảnh sử dụng HKC được tính theo biểu thức sau:

$$L = 2L_1 = 2(y'_2 + y'_4). \quad (3.12)$$

Từ (3.11) và (3.12) ta được điều phải chứng minh.

Áp dụng định lý 3.3, chúng ta có thể xây dựng thuật toán phát hiện ảnh có giấu tin bằng kỹ thuật HKC và ước lượng thông tin giấu trong ảnh sau:

### **Thuật toán 3.3 - Phát hiện và ước lượng độ dài $M$ của ảnh\_stego\_HKC**

**Đầu vào:** Một ảnh 8 – bit cấp độ màu C

**Đầu ra:** Kiểm tra xem ảnh C có giấu tin sử dụng kỹ thuật giấu HKC hay không.  
Nếu có cho biết lượng bit đã giấu trong ảnh.

**Bước 1:** Thống kê tần suất các điểm ảnh được  $\{h_i\}_{i=0}^{255}$ . Tìm điểm Peak có tần suất lớn nhất được cặp  $(x_{\max}, y_{\max})$  với  $x_{\max} = \text{Peak}$ ,  $y_{\max} = h_{\text{peak}}$ .

**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  $(x_{\max+1}, y_{\max+1})$ ,  $(x_{\max+2}, y_{\max+2})$  của Peak.

**Bước 3.** Nếu năm 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 (3.7) và (3.8) thì kết luận ảnh C có giấu tin với lượng bit thông tin được tính theo (3.9). Ngược lại, có thể kết luận ảnh này không giấu tin bằng HKC.

Áp dụng thuật toán cho thử nghiệm trong phần 3.1.1 trên ảnh Lena.bmp cấp xám 8-bit, thông tin giấu là ảnh Logo.bmp nhị phân kích cỡ  $128 \times 56$  điểm ảnh (tương ứng 7146 bit), chúng ta ước lượng xấp xỉ số độ dài bit thông tin đã giấu trong ảnh  $L = 7148$  bit.

### 3.1.3. Các kết quả thử nghiệm

#### 3.1.3.1. Thử nghiệm

*Tập ảnh thử nghiệm:* Tập ảnh thử nghiệm là tập  $\mathcal{C}_0$  gồm 2088 ảnh đã giới thiệu nguồn gốc trong 1.3.2.

*Thử nghiệm:* Để đánh giá và so sánh hiệu quả của ba kỹ thuật phát hiện: Kỹ thuật của Kuo và Lin, kỹ thuật của Kuo và Lin được cải tiến và kỹ thuật do luận án đề xuất, luận án thực hiện các thực nghiệm với hai trường hợp sau:

#### 1/. Trường hợp 1 (giấu cùng một lượng bit thông tin)

Tập ảnh  $\mathcal{C}_0$  được giấu cùng một thông tin với độ dài bit thông tin là 2500 bit (bit thông tin được sinh ngẫu nhiên) bằng kỹ thuật giấu HKC được tập ảnh đã giấu tin  $\mathcal{S}_{\text{HKC}_{2500}}$  gồm 2088 ảnh. Sử dụng ba kỹ thuật phát hiện ảnh có giấu tin HKC để phân loại các ảnh gốc và ảnh có giấu tin bằng HKC trong hai tập  $\mathcal{C}_0$  và  $\mathcal{S}_{\text{HKC}_{2500}}$  ta được kết quả phân loại trong bảng 3.1.

**Bảng 3.1. Bảng kết quả phân loại trên tập  $\mathcal{C}_0$  và  $\mathcal{S}_{\text{HKC}_{2500}}$**

| Tập ảnh<br>Kỹ thuật phát hiện    | Tập ảnh $\mathcal{C}_0$                 |          | Tập ảnh $\mathcal{S}_{\text{HKC}_{2500}}$ |          |
|----------------------------------|---|----------|---|----------|
|                                  | Số ảnh phát hiện được với từng loại ảnh |          |   |          |
|                                  | Gốc                                     | Giấu tin | Gốc                                       | Giấu tin |
| Kỹ thuật của Kuo và Lin          | 2076                                    | 12       | 2085                                      | 3        |
| Kỹ thuật của Kuo và Lin cải tiến | 1776                                    | 312      | 212                                       | 1876     |
| Kỹ thuật phát hiện đề xuất       | 1950                                    | 138      | 38  | 2050     |

Đánh giá kết quả trong bảng 3.1 theo độ đo P sử dụng (1.3), R sử dụng (1.4), F sử dụng (1.6) trên tập ảnh  $\mathcal{V}$  gồm 4176 ảnh trong đó 2088 ảnh của tập  $\mathcal{C}_0$  và 2088 ảnh của tập  $\mathcal{S}_{\text{HKC}_{2500}}$  ta được kết quả trong bảng 3.2.

**Bảng 3.2. Kết quả đánh giá bằng các độ đo P, R, F trên tập ảnh  $\mathcal{V}$  gồm 4176 ảnh ( $\mathcal{C}_0$  và  $\mathcal{S}_{HKC\_2500}$ )**

| Kỹ thuật \ Độ đo                     | P     | R    | F     |
|--------------------------------------|-------|------|-------|
| Kỹ thuật phát hiện của Kuo và Lin    | 0.001 | 0.2  | 0.002 |
| Kỹ thuật của Kuo và Lin có chỉnh sửa | 0.89  | 0.82 | 0.85  |
| Kỹ thuật phát hiện đề xuất           | 0.98  | 0.94 | 0.96  |

*Ước lượng thông tin giấu:* Tiến hành ước lượng số bit thông tin giấu trên tập ảnh  $\mathcal{C}_0$  và tập ảnh  $\mathcal{S}_{HKC\_2500}$  ta được kết quả tương ứng trong bảng 3.3.

**Bảng 3.3. Kết quả ước lượng thông tin giấu trên tập  $\mathcal{C}_0$  và  $\mathcal{S}_{HKC\_2500}$**

| Tập ảnh thử nghiệm        | Độ dài bit trung bình ước lượng | Độ lệch |
|---------------------------|---------------------------------|---------|
| $\mathcal{C}_0$           | 386.37                          | 1214.89 |
| $\mathcal{S}_{HKC\_2500}$ | 2494.357                        | 2116.37 |

Từ bảng 3.3 ta thấy, với tập ảnh gốc  $\mathcal{C}_0$  kết quả ước lượng trung bình độ dài bit thông tin là 386.37 với độ lệch 1214.89 là do trong tập ảnh  $\mathcal{C}_0$  chương trình phát hiện ra sai 138 ảnh gốc là ảnh có giấu tin, nó sẽ ước lượng giá trị số bit thông tin của 138 ảnh này làm cho số bit trung bình trên 2088 ảnh gốc là rất lớn. Còn với tập ảnh  $\mathcal{S}_{HKC\_2500}$  với lượng giấu thực tế là 2500 bit nhưng chương trình ước lượng được trung bình là 2494.357 là do nó phát hiện sai 138 ảnh là gốc vì vậy giá trị bit dữ liệu giấu ước lượng trung bình thấp hơn giá trị bit đã giấu trong tập ảnh.

## 2/. Trường hợp 2 (các ảnh được giấu với lượng thông tin giấu lớn nhất)

Tập ảnh  $\mathcal{C}_0$  được giấu một lượng bit thông tin (bit thông tin được sinh ngẫu nhiên) với tỉ lệ giấu lớn nhất (khả năng giấu cho phép của mỗi ảnh) bằng kỹ thuật giấu HKC được tập ảnh đã giấu tin  $\mathcal{S}_{HKC\_R100}$  gồm 2088 ảnh. Sử dụng ba kỹ thuật phát hiện ảnh có giấu tin HKC để phân loại các ảnh gốc và ảnh có giấu tin trong hai tập  $\mathcal{C}_0$  và  $\mathcal{S}_{HKC\_R100}$  ta được kết quả trong bảng 3.4.



**Bảng 3.4. Bảng kết quả phân loại bằng ba kỹ thuật phát hiện: của Kuo và Lin, của Kuo và Lin cải tiến và kỹ thuật đề xuất mới trên tập  $\mathcal{S}_{HKC\_R100}$**

| Tập ảnh<br>Kỹ thuật phát hiện    | Tập ảnh $\mathcal{S}_{HKC\_R100}$ |              |
|----------------------------------|-----------------------------------|--------------|
|                                  | ảnh gốc                           | ảnh giấu tin |
| Kỹ thuật của Kuo và Lin          | 312                               | 288          |
| Kỹ thuật của Kuo và Lin cải tiến | 95                                | 505          |
| Kỹ thuật phát hiện đề xuất       | 16                                | 584          |

Đánh giá kết quả trong bảng 3.4 theo độ đo P, R, F trên tập ảnh  $\mathbf{U}$  gồm 4176 ảnh trong đó 2088 ảnh của tập  $\mathcal{C}_0$  và 2088 ảnh của tập  $\mathcal{S}_{HKC\_R100}$  ta được kết quả trong bảng 3.5.

**Bảng 3.5. Kết quả đánh giá bằng các độ đo P, R, F trên tập ảnh  $\mathbf{U}$  gồm 4176 ảnh ( $\mathcal{C}_0$  và  $\mathcal{S}_{HKC\_R100}$ )**

| Độ đo<br>Kỹ thuật                 | P    | R    | F    |
|-----------------------------------|------|------|------|
| Kỹ thuật phát hiện của Kuo và Lin | 0.64 | 0.99 | 0.78 |
| Kỹ thuật của Kuo và Lin cải tiến  | 0.89 | 0.82 | 0.85 |
| Kỹ thuật phát hiện đề xuất        | 0.98 | 0.94 | 0.96 |

### 3.1.3.2. Nhận xét

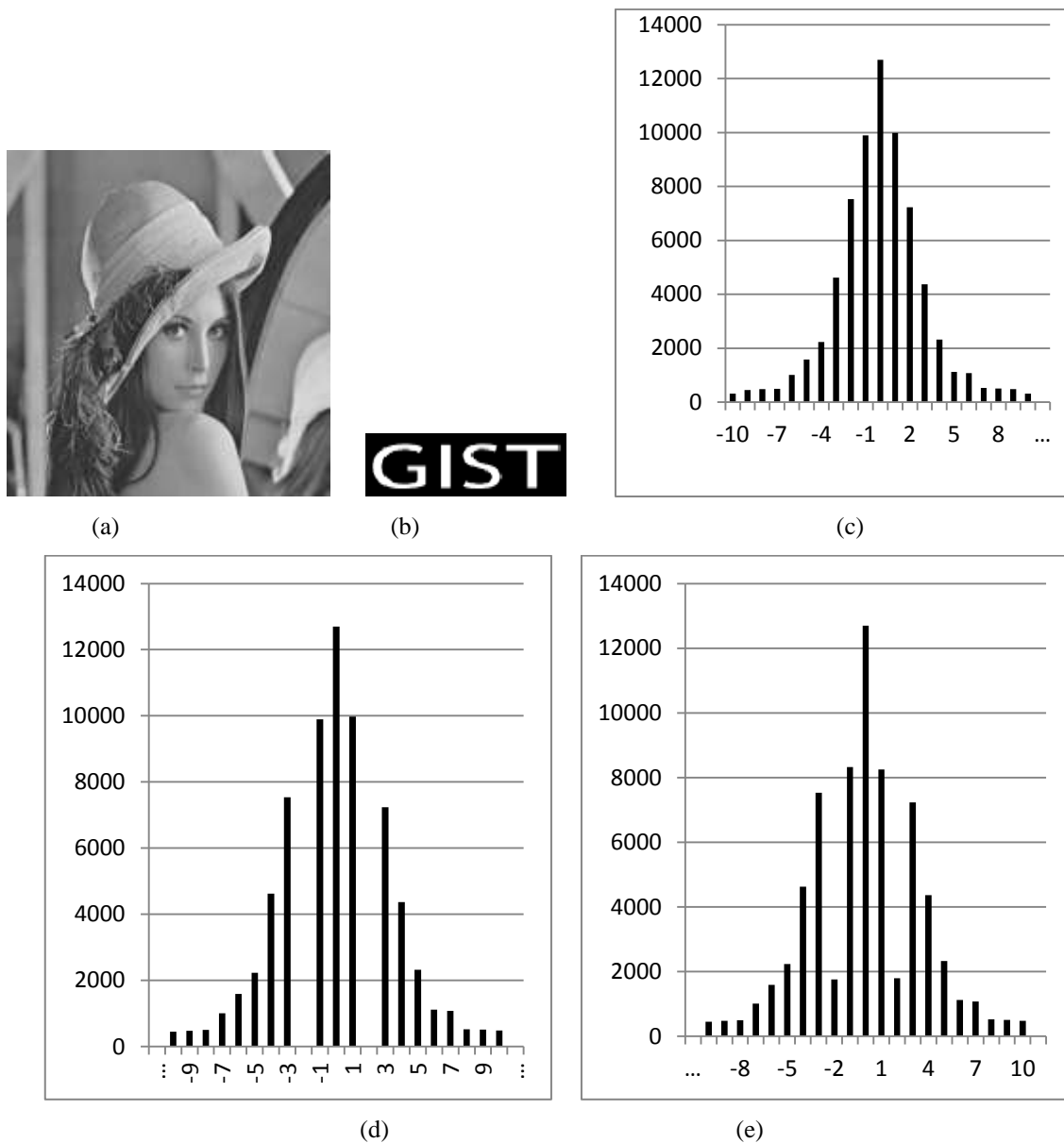
Từ kết quả trong các bảng 3.1 - 3.6 luận án đưa ra một số nhận xét sau:

- Đối với trường hợp phân loại ảnh gốc: kỹ thuật phát hiện của Kuo và Lin tốt hơn kỹ thuật cải tiến và kỹ thuật đề xuất.
- Đối với các ảnh được giấu với lượng thông tin giấu thấp (so với khả năng giấu lớn nhất của ảnh) thì kỹ thuật của Kuo và Lin phát hiện không tốt như đã phân tích ở trên, kỹ thuật cải tiến phát hiện tốt hơn.
- Đối với tập ảnh giấu tin với lượng thông tin giấu lớn nhất thì kỹ thuật của Kuo và Lin được cải tiến và kỹ thuật đề xuất cho kết quả phân loại tốt hơn.
- Kỹ thuật đề xuất cho kết quả phân loại như nhau trong cả hai trường hợp.

## 3.2. PHÁT HIỆN ẢNH CÓ GIẤU TIN SỬ DỤNG KỸ THUẬT GIẤU DIH

### 3.2.1. Tóm lược kỹ thuật giấu tin DIH

Kỹ thuật giấu tin thuận nghịch dựa trên biểu đồ sai phân ảnh DIH (Difference Image Histogram) do Lee và các cộng sự đề xuất năm 2004 [49]. Ý tưởng của kỹ thuật này là nhúng thông tin dựa vào hệ số sai phân trong ảnh. Giả sử dữ liệu ảnh gốc 8 – bit Lena.bmp (hình 3.4. (a)) kích cỡ  $m \times n$  điểm ảnh được biểu diễn bằng vector  $\{x_{tk}\}$  với  $t=0, \dots, m-1, k=0, \dots, n-1, x_{tk} \in \{0, \dots, 255\}$ , khi đó các hệ số sai phân  $\{d_{ij}\}$  của ảnh được tính theo  $d_{ij} = x_{i,2j+1} - x_{i,2j}$  với  $0 \leq i \leq m-1, 0 \leq j \leq n/2 - 1$ . Tính tần suất của các hệ số sai phân được vector  $h_d$  (với biểu đồ hình 3.4 (c)). Nhóm tác giả thấy rằng các giá trị tần suất tập trung phần lớn vào các hệ số sai phân có giá trị -2, -1, 0, 1, 2, do đó có thể giấu thông tin dựa vào các hệ số sai phân này. Để giấu tin có thể khôi phục lại ảnh gốc, họ sẽ phải dịch chuyển các cột tần suất có hệ số  $d_{ij}$  lớn hơn 1 và nhỏ hơn -1 để làm rộng các cột tần suất các hệ số bằng 2 và -2 (hình 3.4 (d)). Sau đó chuỗi thông tin  $M$  (ví dụ là dữ liệu của ảnh nhị phân (hình 3.4 (b)) kích cỡ 128x56 điểm ảnh) sẽ được giấu vào các điểm ảnh mà hệ số sai phân của nó sau khi chỉnh sửa có giá trị là 1 hoặc -1 theo nguyên tắc: xét từng cặp điểm ảnh  $(x_{i,2j}, x_{i,2j+1})$  (theo thứ tự nào đó), nếu  $d_{ij}$  của cặp này có giá trị 1 hoặc -1, ta kiểm tra  $b \in M$  cần giấu  $b=1$  thì  $x_{i,2j}$  tăng lên 1 (nếu  $d_{ij}=1$ ) hoặc  $x_{i,2j}$  giảm 1 (nếu  $d_{ij}=-1$ ), còn nếu  $b=0$  các giá trị vẫn giữ nguyên (mặc định coi như đã giấu thông tin vào  $d_{ij}$ ). Quá trình giấu này thực chất là dịch chuyển một phần cột hệ số sai phân -1, 1 sang hệ số -2, 2. Sau khi giấu tin được biểu đồ tần suất sai phân mới (hình 3.4 (e)).



Hình 3.4. (a) Ảnh Lena.bmp, (b) thông tin cần giấu là ảnh nhị phân kích cỡ 128 x 56 điểm ảnh, các biểu đồ sai phân: (c) ảnh Lena (gốc), (d) khi dịch chuyển, (e) sau khi giấu tin.

### 3.2.2. Phương pháp phát hiện ảnh có giấu tin sử dụng kỹ thuật giấu DIH

#### 3.2.2.1. Phân tích kỹ thuật giấu DIH

Kỹ thuật giấu DIH là một trường hợp riêng của kỹ thuật giấu trên LSB theo phương pháp tăng giảm LSB. Theo quá trình giấu tin trong 3.2.1, chúng ta thấy rằng kỹ thuật giấu DIH chỉ giấu được một lượng tin rất thấp, khả năng giấu phụ thuộc vào giá trị tần suất sai phân bằng 1 và -1. Theo ví dụ trong 3.2.1 thì khả năng giấu số bit lớn nhất của ảnh Lena là  $L = h_{-1} + h_1 = 19877$  (tương đương với tỉ lệ giấu lớn

nhất  $R_{\max}=7.58\%$  miền LSB của ảnh). Đây là tỉ lệ giấu làm thay đổi rất ít nội dung của ảnh gốc vì theo nhóm tác giả giới thiệu kỹ thuật này đưa ra bằng phép đo  $PSNR>51dB$ .

Chúng ta sử dụng một số phương pháp phát hiện mù trên LSB trong chương 2 để phát hiện ảnh có giấu tin bằng kỹ thuật giấu DIH như sau: sử dụng tập ảnh  $\mathcal{C}$  (600 ảnh lấy ra từ tập ảnh gốc  $\mathcal{C}_0$ ) cùng giấu thông tin là dữ liệu ảnh nhị phân (hình 3.4. (b)) kích cỡ  $128 \times 56$  điểm ảnh (tương ứng với chuỗi 7168 bit) được tập ảnh  $\mathcal{S}_{DIH_{7168}}$ . Sau đó sử dụng một số kỹ thuật phát hiện tổng quát LSB cho tập ảnh  $\mathcal{S}_{DIH_{7168}}$  được kết quả phát hiện trong bảng 3.6.

**Bảng 3.6. Sử dụng kỹ thuật phát hiện tổng quát trên miền LSB để phân loại ảnh trên tập  $\mathcal{S}_{DIH_{7168}}$**

|              | “Độ lệch chuẩn” | $\chi^2$ | “Tỉ lệ xám” | $\chi_n^2$ [95] | LLRT [80] |
|--------------|-----------------|----------|-------------|-----------------|-----------|
| Ảnh gốc      | 462             | 582      | 406         | 595             | 297       |
| Ảnh giấu tin | 138             | 18       | 194         | 5               | 303       |

Để kiểm tra bằng phương pháp ước lượng thông tin giấu trên LSB của ảnh, luận án sử dụng ảnh Lena.bmp (hình 3.4 (a)) giấu một lượng thông tin là dữ liệu ảnh nhị phân (hình 3.4. (b)) kích cỡ  $128 \times 56$  điểm ảnh (tương ứng với chuỗi 7168 bit) ứng với tỉ lệ 2.73 % miền LSB của ảnh. Sử dụng kỹ thuật ước lượng RS, DI, “Trùng khớp” ta được kết quả ước lượng trong bảng 3.7.

**Bảng 3.7. Ước lượng thông tin giấu cho ảnh Lena.bmp trước và sau khi giấu tin sử dụng DIH bằng kỹ thuật ước lượng thông tin trên miền LSB: RS, DI, “Trùng khớp”**

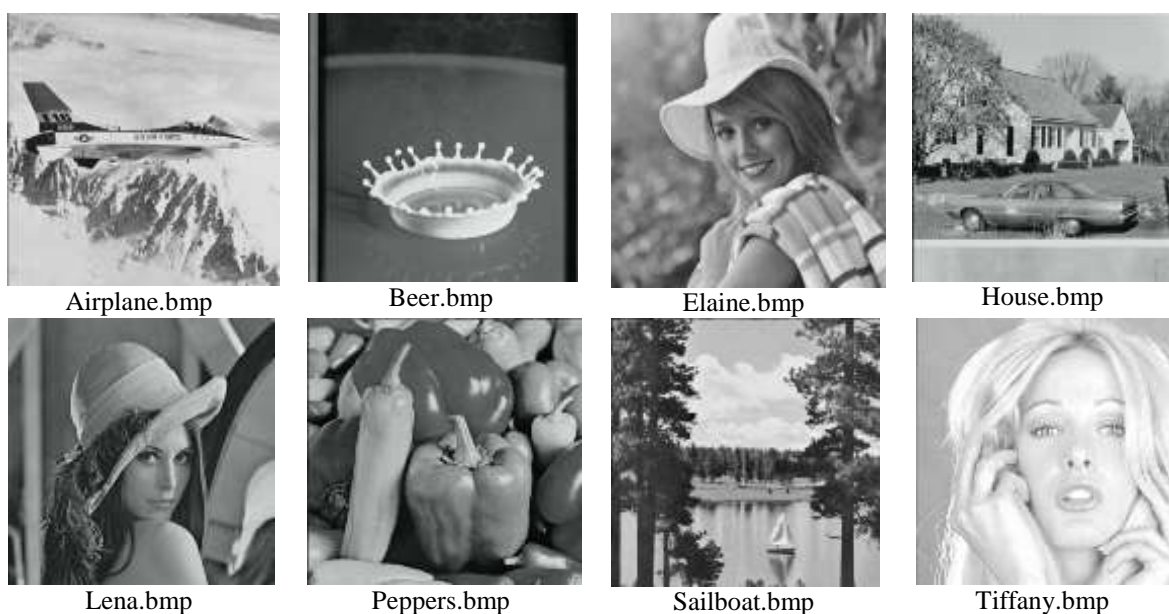
| Lena.bmp           | RS [31]    | DI [102] | “trùng khớp” |
|--------------------|------------|----------|--------------|
| Trước khi giấu tin | R = 0.15 % | R = 12 % | R = 0.037 %  |
| Sau khi giấu tin   | R = 6.36 % | R = 9 %  | R = 3 %      |

Từ hai bảng kiểm tra 3.6 và 3.7 có thể thấy rằng đa số kỹ thuật phát hiện tổng quát trên LSB chỉ phát hiện tốt với tỉ lệ giấu cao còn trong trường hợp này tỉ lệ giấu so với kích cỡ của ảnh là quá nhỏ (7168 bit chỉ bằng từ 2 đến 3% miền LSB

của ảnh). Vì vậy dựa vào phân tích đặc trưng của tập ảnh gốc và ảnh sau khi giấu tin sử dụng kỹ thuật giấu DIH luận án này đưa ra phương pháp phát hiện tối ưu hơn và có thể ước lượng thông tin đã giấu trong ảnh trong mục tiếp theo.

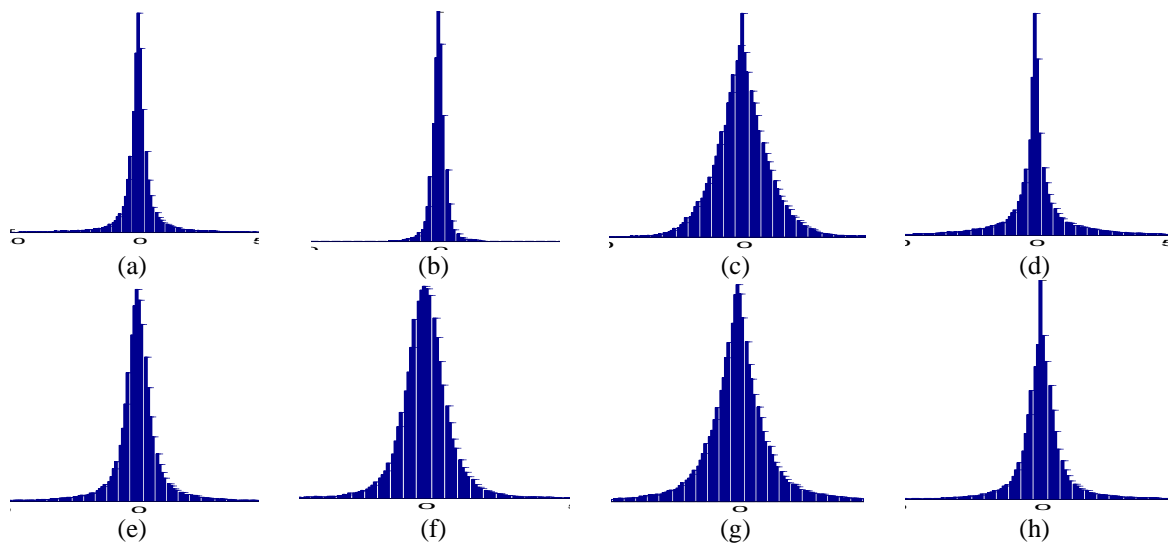
### 3.2.2.2. Phương pháp phát hiện và ước lượng thông tin giấu

Để đưa ra phương pháp phát hiện phù hợp với kỹ thuật giấu DIH, trước tiên chúng ta đưa ra phân tích trên một tập gồm 8 ảnh 8-bit kích cỡ 512x512 điểm ảnh tải về từ thư viện ảnh [107] với nội dung trong hình 3.5.



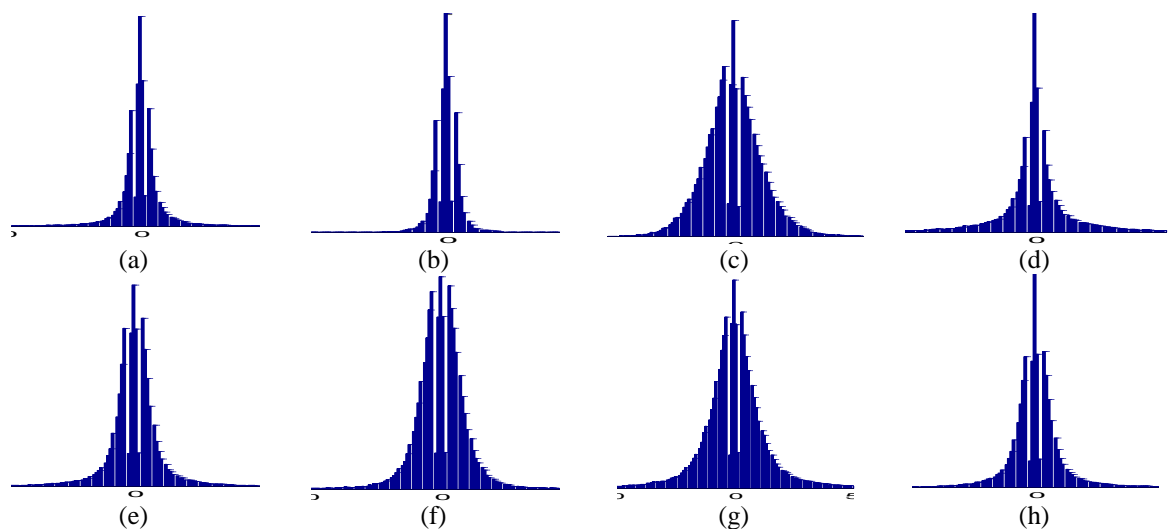
Hình 3.5. Tập ảnh thử nghiệm

Tính tần suất các hệ số sai phân của từng ảnh ta được biểu đồ tần suất tương ứng trên từng ảnh theo hình 3.6.



Hình 3.6. Biểu đồ tần suất hệ số sai phân của ảnh trước khi giấu tin bằng DIH: a) *Airplane.bmp*, b) *Beer.bmp*, c) *Elaine.bmp*, d) *House.bmp*, e) *Lena.bmp*, f) *Peppers.bmp*, g) *Sailboat.bmp*, h) *Tiffany.bmp*

Sau đó tập ảnh này được giấu cùng một thông tin là ảnh nhị phân kích cỡ  $128 \times 56$  điểm ảnh (hình 3.4. b) bằng kỹ thuật giấu DIH được tập ảnh có giấu tin. Tính tần suất các hệ số sai phân của ảnh ta có biểu đồ tần suất của từng ảnh theo hình 3.7.



Hình 3.7. Biểu đồ tần suất hệ số sai phân của ảnh sau khi giấu tin bằng DIH: a) *Airplane.bmp*, b) *Beer.bmp*, c) *Elaine.bmp*, d) *House.bmp*, e) *Lena.bmp*, f) *Peppers.bmp*, g) *Sailboat.bmp*, h) *Tiffany.bmp*

Từ hình 3.6 và 3.7 chúng ta thấy, đối với ảnh không giấu tin thì biểu đồ tần suất  $h$  của các hệ số sai phân  $d$  có phân bố Gaussian với hàm mật độ xác suất: [90].

$$p_{v,\beta}(x) = \frac{v}{2\beta\Gamma\frac{1}{v}} \exp\left\{-\left(\frac{|x|}{\beta}\right)^v\right\}$$

Hay mối quan hệ của các  $h_i$  như sau trong ảnh gốc:

$$h_1 + h_{-1} > h_2 + h_{-2} > h_3 + h_{-3} > \dots > h_{10} + h_{-10} > \dots$$

Còn đối với ảnh có giấu tin thì:

$$h_1 + h_{-1} > h_2 + h_{-2}, h_2 + h_{-2} \leq h_3 + h_{-3}.$$

Sự thay đổi này là do kỹ thuật giấu DIH tạo ra, nó thay đổi tần suất  $h_{\pm 2}$  của ảnh để giấu thông tin. Đây chính là vấn đề mấu chốt để phát hiện ảnh có giấu tin bằng DIH. Từ đó chúng ta có thể ước lượng được xấp xỉ thông tin đã giấu dựa vào  $h_{\pm 2}$ . Vì thông tin đem giấu là một chuỗi bit có phân bố độc lập nên xác suất số bit “0” xuất hiện trong chuỗi thông tin xấp xỉ bằng xác suất số bit “1” và bằng 0.5 ( $p(0) = p(1) = 0.5$ ). Vì vậy  $\frac{1}{2}$  chuỗi thông tin sẽ được giấu trong  $h_{+1}$  và phần còn lại được giấu trong  $h_{+2}$ , do đó độ dài xấp xỉ bit thông tin đem giấu được tính như sau:  $L = 2*(h_{-2} + h_2)$

Từ các phân tích trên chúng ta đưa ra định lý 3.4 về mối quan hệ tần suất của các hệ số sai phân trong ảnh có giấu tin và ước lượng độ dài bit thông tin giấu trong ảnh như sau:

*Định lý 3.4 - Có 2 cặp giá trị  $(h_2, h_{-2}), (h_3, h_{-3})$  được chọn từ vector tần suất các hệ số sai phân của một ảnh. Khi đó ảnh có giấu tin bằng DIH nếu mối quan hệ của 2 cặp giá trị này thỏa mãn:*

$$\frac{h_2+h_{-2}}{h_3+h_{-3}} \leq T \tag{3.13}$$

và lượng bit thông tin đã giấu được tính bằng biểu thức:

$$L = 2*(h_{-2} + h_2) \tag{3.14}$$

Với  $T$  là ngưỡng để phân loại.

Chứng minh:

Theo [49] kỹ thuật giấu tin DIH chủ yếu làm thay đổi các cột tần suất hệ số sai phân  $h_2, h_{-2}, h_3, h_{-3}$ . Đối với ảnh không giấu tin thì biểu đồ tần suất  $h$  của các hệ số sai phân  $d$  có phân bố Gaussian, hay mối quan hệ của các  $h_i$  như sau:

$$h_1 > h_2 > h_3 > h_4 > \dots$$

$$h_{-1} > h_{-2} > h_{-3} > h_{-4} > \dots$$

$$\text{hay } \frac{h_2 + h_{-2}}{h_3 + h_{-3}} > T$$

Còn đối với ảnh có giấu tin thì:

$$h_2 < h_3$$

$$h_{-2} < h_{-3}$$

$$\text{hay } \frac{h_2 + h_{-2}}{h_3 + h_{-3}} \leq T, T \text{ là giá trị ngưỡng} \quad (3.15)$$

(vì trước khi giấu cột tần suất  $h_2$  được dịch chuyển sang  $h_3$ ,  $h_3$  chuyển sang  $h_4$ , ... làm rộng cột tần số  $h_2$  sau đó một phần  $h_1$  được chuyển sang  $h_2$  để giấu tin. Tương tự với các cột tần suất của hệ số sai phân có giá trị âm)

Từ đó chúng ta có thể ước lượng được xấp xỉ thông tin đã giấu dựa vào  $h_{\pm 2}$ . Vì thông tin đem giấu là một chuỗi bit có phân bố độc lập nên xác suất số bit “0” xuất hiện trong chuỗi thông tin xấp xỉ bằng xác suất số bit “1” và bằng 0.5 ( $p(0) = p(1) = 0.5$ ). Vì vậy  $\frac{1}{2}$  chuỗi thông tin sẽ được giấu trong  $h_{\pm 1}$  và phần còn lại được giấu trong  $h_{\pm 2}$ , do đó độ dài xấp xỉ của thông tin đem giấu được tính như sau:

$$L = 2 * (h_{-2} + h_2) \quad (3.16)$$

Từ (3.15) và (3.16) ta được điều phải chứng minh

Từ đó ta có thuật toán phát hiện dựa vào định lý 3.4 như sau:



### **Thuật toán 3.4 – Phát hiện ảnh stego\_DIH**

**Đầu vào :** Ảnh C cần kiểm tra

**Đầu ra:** Kết luận ảnh C có giấu tin bằng DIH hay không

**Bước 1.** Tính giá trị sai phân  $d$  giữa các cặp điểm ảnh giống như quy trình giấu tin.

Sau đó tính tần suất của hệ số sai phân này, ký hiệu là  $h_i$ .

**Bước 2.** So sánh tỷ lệ giữa  $h_{\pm 2}$  và  $h_{\pm 3}$  nếu thỏa mãn (3.13) thì thực hiện bước 3.

Ngược lại, thực hiện bước 4.

**Bước 3.** Ảnh có giấu tin. Ước lượng độ dài thông tin giấu  $L$  theo biểu thức (3.14).

**Bước 4.** Ảnh không giấu tin

Dựa vào tập ảnh thực nghiệm (trên 2088 ảnh) cho thấy  $T=1$  cho kết quả tốt.

Áp dụng thuật toán cho thử nghiệm trong phần 3.2.1 trên ảnh Lena.bmp giấu thông tin là ảnh Logo.bmp nhị phân kích cỡ  $128 \times 56$  điểm ảnh (tương ứng 7146 bit), chúng ta ước lượng được độ dài bit dữ liệu đã trong ảnh  $L = 7142$  bit.

### **3.2.3. Các kết quả thử nghiệm**

#### **3.2.3.1. Thử nghiệm**

*Tập ảnh thử nghiệm:* Tập ảnh thử nghiệm là tập ảnh  $\mathcal{C}_0$  gồm 2088 ảnh.

*Giấu tin:* Tập  $\mathcal{C}_0$  được giấu cùng một chuỗi thông tin có độ dài 6000 bit (chuỗi được sinh ngẫu nhiên) bằng kỹ thuật giấu DIH được tập ảnh mới  $\mathcal{S}_{\text{DIH}_{6000}}$ .

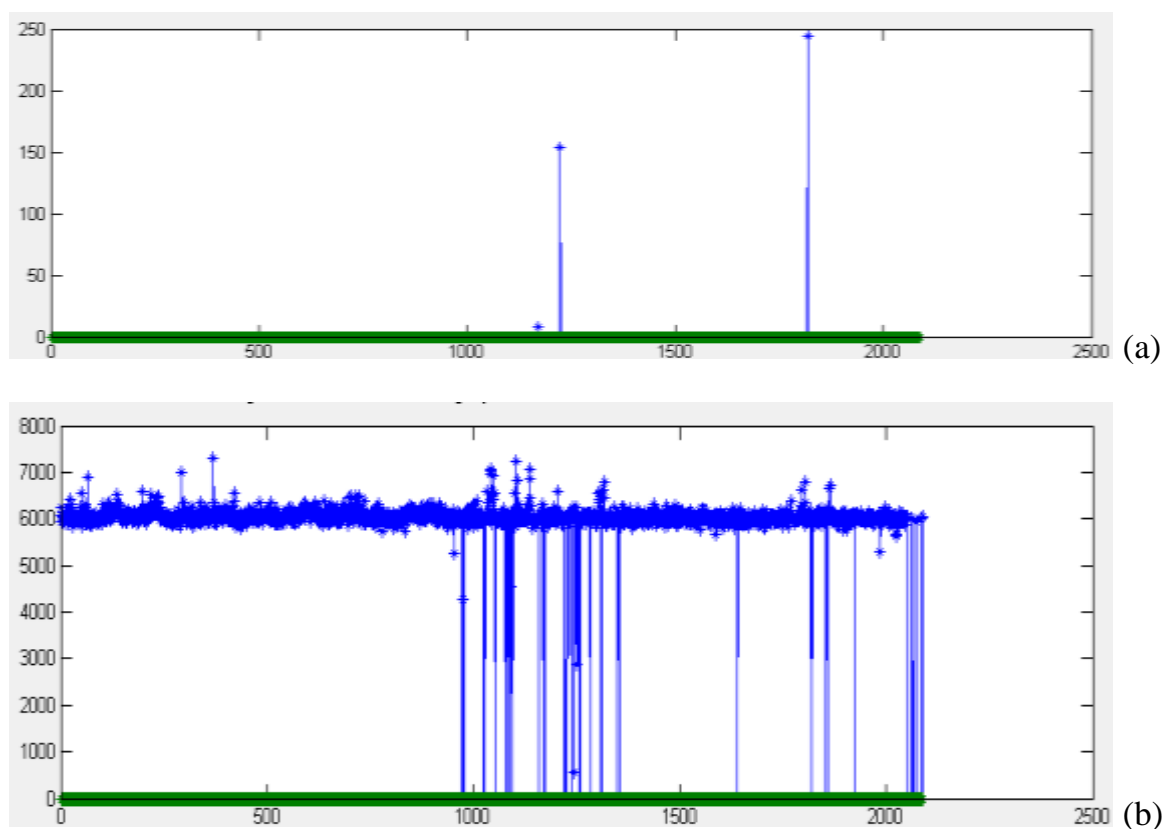
*Phân loại ảnh:* Sử dụng kỹ thuật phát hiện ảnh có giấu tin bằng DIH cho hai tập ảnh  $\mathcal{C}_0$  và  $\mathcal{S}_{\text{DIH}_{6000}}$  ta được kết quả trong bảng 3.8 (tương ứng với hình 3.8).

**Bảng 3.8. Bảng kết quả phân loại ảnh có giấu tin bằng DIH trên tập  $\mathcal{C}_0$  và  $\mathcal{S}_{\text{DIH}_{6000}}$**

| Tập ảnh thử nghiệm                | Số ảnh phát hiện được với từng loại ảnh |             |
|-----------------------------------|---|-------------|
|                                   | Gốc                                     | Có giấu tin |
| $\mathcal{C}_0$                   | 2085                                    | 3           |
| $\mathcal{S}_{\text{DIH}_{6000}}$ | 72                                      | 2016        |

Đánh giá kết quả trong bảng 3.8 theo độ đo P, R, F trên tập ảnh  $\mathcal{W}$  gồm 4176 ảnh trong đó 2088 ảnh của tập  $\mathcal{C}_0$  và 2088 ảnh của tập  $\mathcal{S}_{\text{DIH}_{6000}}$  ta được kết quả  $P = 0.97$ ,  $R = 0.99$ ,  $F = 0.98$ .

Ước lượng thông tin giầu: trong hai tập ảnh  $\mathcal{C}_0$  và  $\mathcal{S}_{\text{DIH}_{6000}}$  ta được kết quả ước lượng trong hình 3.8 ứng với bảng 3.9.



Hình 3.8. Kết quả ước lượng độ dài thông tin giầu: a) trên tập ảnh  $\mathcal{C}_0$ , b) trên tập  $\mathcal{S}_{\text{DIH}_{6000}}$

**Bảng 3.9. Kết quả ước lượng thông tin giầu trên tập  $\mathcal{C}_0$  và  $\mathcal{S}_{\text{DIH}_{6000}}$**

| Tập ảnh thử nghiệm                | Độ dài bit trung bình ước lượng | Độ lệch |
|-----------------------------------|---------------------------------|---------|
| $\mathcal{C}_0$                   | 0.194                           | 6.315   |
| $\mathcal{S}_{\text{DIH}_{6000}}$ | 5837.31                         | 1122.07 |

### 3.2.3.2. Nhận xét

Từ bảng kết quả phân loại 3.8 và bảng ước lượng thông tin 3.9 trên hai tập ảnh  $\mathcal{C}_0$  và  $\mathcal{S}_{\text{DIH}_{6000}}$ , luận án chỉ ra rằng:

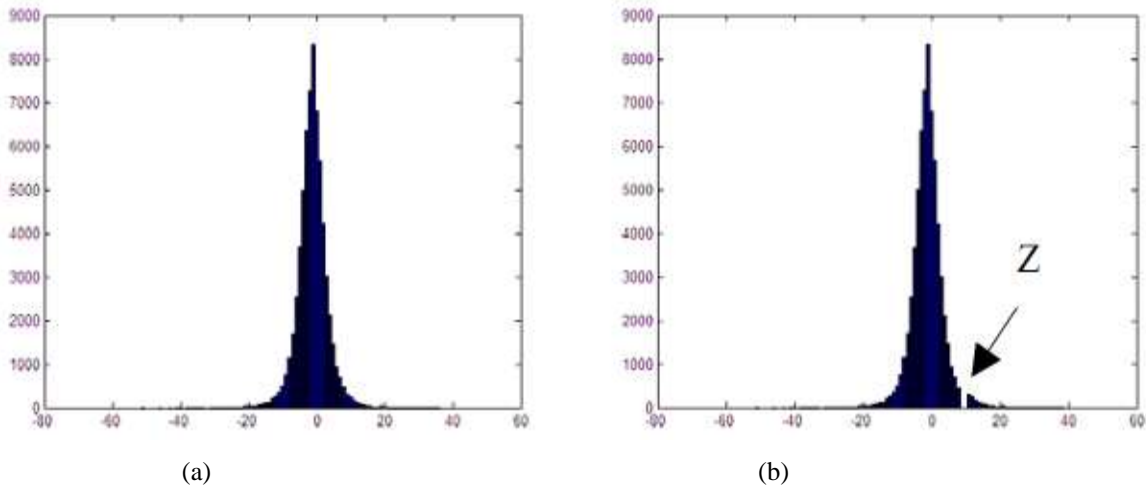
- Phương pháp phát hiện đề xuất cho ảnh có giấu tin bằng DIH với độ tin cậy cao và sai số loại I nhỏ (0.03) với tập ảnh có số lượng ảnh lớn.
- Phương pháp phát hiện này cho kết quả tối ưu hơn phương pháp phát hiện mù trên LSB.
- Tuy nhiên, ước lượng có chệch với các ảnh có độ nhiễu cao như ước lượng chỉ ra trong hình 3.8 (các ảnh được đánh số từ 993 đến 2088, các ảnh này là các ảnh được chụp từ máy ảnh kỹ thuật số và điện thoại di động).

## 3.3. PHÁT HIỆN ẢNH CÓ GIẤU TIN SỬ DỤNG KỸ THUẬT GIẤU IWH

### 3.3.1. Tóm lược kỹ thuật giấu tin IWH

Cũng xuất phát từ yêu cầu khôi phục xấp xỉ ảnh gốc sau khi tách thông tin, vào năm 2006, Xuan và các đồng nghiệp đề xuất kỹ thuật giấu IWH (Integer Wavelet Histogram) [99]. Kỹ thuật này có ý tưởng gần giống kỹ thuật giấu tin DIH, tuy nhiên sự khác nhau ở chỗ: thay vì dịch chuyển các cột tần suất sai phân, thì họ sử dụng phương pháp dịch chuyển tần suất của các hệ số biến đổi wavelet nguyên với vị trí tùy chọn.

Ban đầu họ thực hiện phép biến đổi Wavelet cho miền không gian ảnh theo chuẩn biến đổi trong kỹ thuật nén JPEG2000 [99, 72] để được bốn băng tần (LL, LH, HL, HH). Thực hiện nhúng thông tin vào ba băng tần cao LH, HL, HH nơi được cho là ít ảnh hưởng đến chất lượng ảnh gốc. Tính tần suất của các hệ số IWT (hình 3.8 (a)), các cột tần suất có giá trị lớn hơn  $Z$  sẽ bị dịch chuyển sang phải, mục đích làm rộng cột tần suất có giá trị  $Z$  (hình 3.9 (b)).



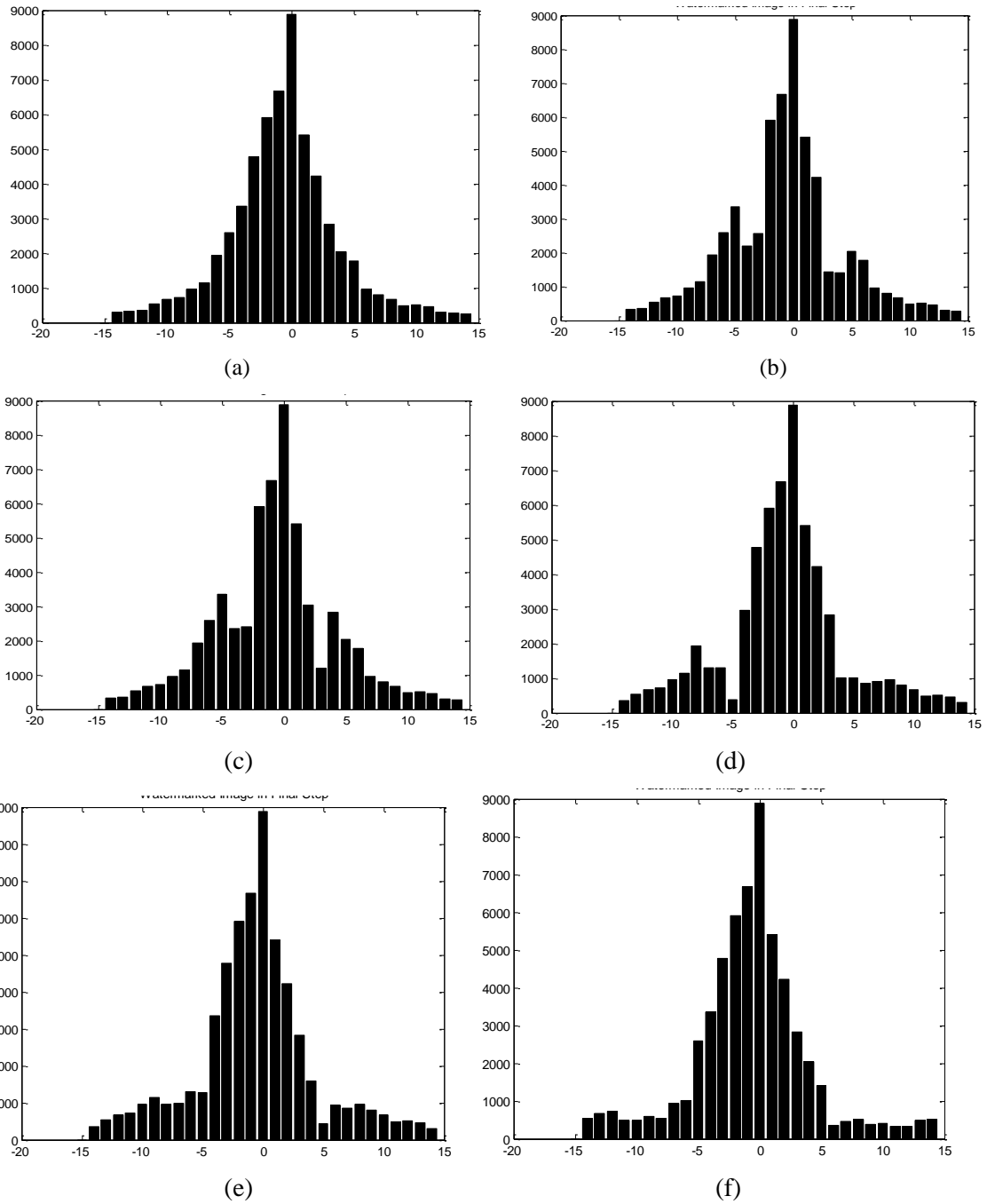
Hình 3.9. Biểu đồ tần suất các hệ số wavelet: (a) Biểu đồ ảnh gốc ban đầu, (b) Biểu đồ sau khi làm rộng một cột tần suất hệ số có giá trị  $Z$  [99].

Thực hiện giấu thông tin, quét toàn bộ các hệ số wavelet trong các băng tần cao, khi gặp một hệ số có giá trị  $Z - 1$ , kiểm tra bit thông tin cần giấu, nếu có giá trị “1” sẽ thực hiện tăng giá trị của hệ số đang xét lên 1, nghĩa là hệ số này sẽ trở thành  $Z$ , nếu bit cần giấu có giá trị “0”, thì hệ số đang xét vẫn được giữ nguyên. Quá trình này lặp lại cho đến khi giấu hết các bit thông tin.

Trong trường hợp số bit cần giấu lớn hơn số hệ số wavelet có giá trị  $Z - 1$ , thì thực hiện tiếp giấu thông tin sang hệ số có giá trị  $-(Z + 1)$  giá trị đối xứng qua cột tần suất có hệ số “0”. Việc thực hiện như sau, ban đầu chúng ta phải làm rộng cột tần số  $-Z$ , sau đó xét các hệ số có giá trị là  $-(Z - 1)$ , nếu bit cần giấu có giá trị “1” thì hệ số này chuyển thành  $-Z$ , ngược lại bit cần giấu có giá trị “0” thì hệ số vẫn giữ nguyên (mặc định coi như đã giấu bit “0” vào hệ số này).

Quá trình lặp lại cho đến khi giấu hết các bit vào trong hệ số  $-Z$ , nếu vẫn còn bit thông tin tiếp tục giấu vào hệ số  $Z - 2$ , cho đến khi giấu xong. Giả sử việc giấu dừng lại ở hệ số có giá trị bằng  $S$  và vị trí cột hệ số bắt đầu giấu tin là  $T$ .

Hình 3.10 là biểu đồ tần suất wavelet của ảnh Lena.bmp sau khi giấu thông tin là ảnh nhị phân kích cỡ  $128 \times 56$  điểm ảnh tương đương với 7168 bit với các vị trí chọn  $T$  ban đầu khác nhau:  $T = 3, T = -3, T = 5, T = -6, T = 8$ .



Hình 3.10. Biểu đồ tần suất hệ số wavelet trên các băng tần cao của: (a) ảnh Lena gốc và ảnh giấu tin với các vị trí ban đầu: (b)  $T = 3$ , (c)  $T = -3$ , (d)  $T = 5$ , (e)  $T = -6$ , (f)  $T = 8$ .

### 3.3.2. Phương pháp phát hiện ảnh có giấu tin sử dụng kỹ thuật giấu IWH

#### 3.3.2.1. Phân tích kỹ thuật giấu IWH

Kỹ thuật giấu IWH là trường hợp riêng của kỹ thuật giấu trên LSB của các hệ số wavelet. Với ảnh chưa giấu thông tin, biểu đồ tần suất của các hệ số wavelet có phân bố Gaussian (với hàm mật độ tính theo (3.6)). Với ảnh có giấu tin, quá trình giấu tin IWH làm phá vỡ phân bố này của biểu đồ tần suất, có thể làm cân bằng một số cặp cột tần suất (hình 3.10 b, c, e, f) hoặc không (hình 3.10 d) tùy thuộc vào ngưỡng được chọn. Do vậy nếu phương pháp phát hiện ảnh có giấu tin trên LSB của các hệ số wavelet dựa vào POV của các cặp hệ số wavelet thường cho độ tin cậy không cao với mọi trường hợp giấu với các ngưỡng chọn T khác nhau, theo thực nghiệm trong 3.3.1 cho ảnh Lena.bmp sau khi giấu lượng thông tin 7168 bit với các ngưỡng chọn T = 3, T = -3, T = 5, T = -6, T = 8 ta được các ảnh giấu tin Lena<sub>3</sub>.bmp, Lena<sub>-3</sub>.bmp, Lena<sub>5</sub>.bmp, Lena<sub>-6</sub>.bmp, Lena<sub>8</sub>.bmp. Sử dụng kỹ thuật phát hiện tổng quát ảnh có giấu tin trên LSB của hệ số wavelet ta được bảng 3.10.

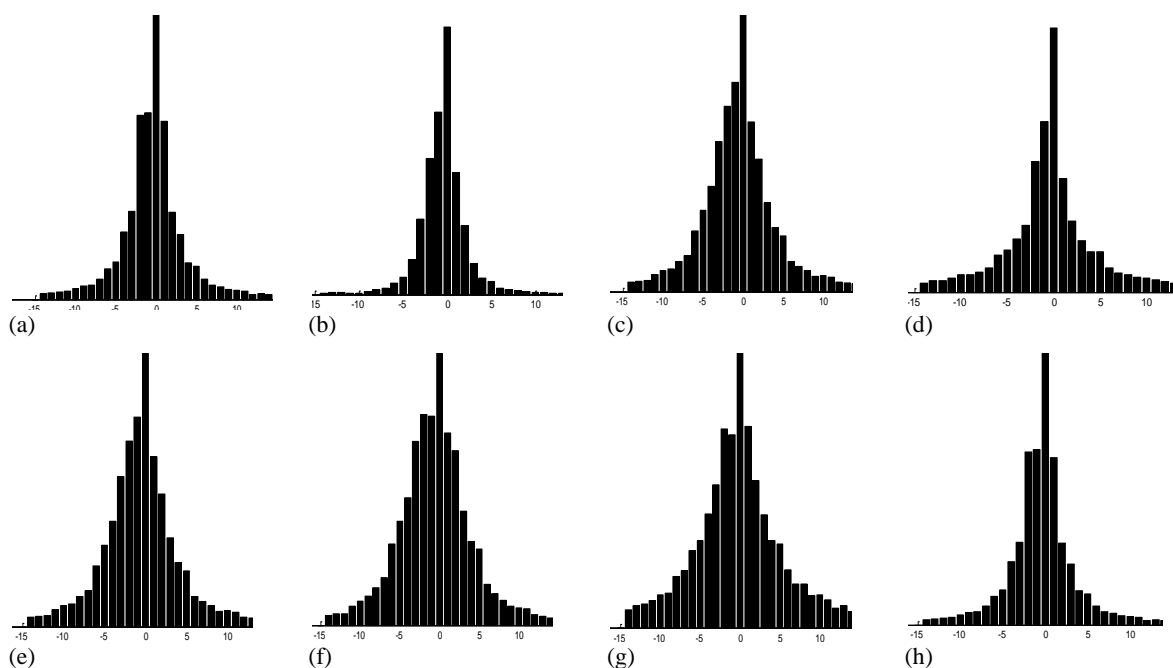
**Bảng 3.10. Kiểm tra ảnh Lena.bmp trước và sau khi giấu tin sử dụng IWH bằng kỹ thuật phát hiện mù trên miền LSB của các hệ số wavelet.**

| Ảnh kiểm tra            | Kỹ thuật phát hiện |                 |
|-------------------------|--------------------|-----------------|
|                         | "Tỉ lệ xám"        | $\chi_n^2 [71]$ |
| Lena.bmp                | Đúng               | Đúng            |
| Lena <sub>3</sub> .bmp  | Đúng               | Sai             |
| Lena <sub>-3</sub> .bmp | Sai                | Đúng            |
| Lena <sub>5</sub> .bmp  | Đúng               | Sai             |
| Lena <sub>-6</sub> .bmp | Đúng               | Đúng            |
| Lena <sub>8</sub> .bmp  | Đúng               | Đúng            |

Đây là tỉ lệ giấu thấp nên các kỹ thuật phát hiện mù cho ảnh giấu trên LSB của các hệ số wavelet cho kết quả không cao. Vì vậy 3.3.2.2 đưa ra phương pháp phát hiện tin cậy hơn so với phương pháp phát hiện tổng quát LSB cho ảnh giấu tin sử dụng kỹ thuật giấu IWH.

### 3.3.2.2. Phương pháp phát hiện và ước lượng thông tin

Để có thể phát hiện và ước lượng thông tin giấu sử dụng kỹ thuật IWH, đầu tiên chúng ta khảo sát biểu đồ tần suất các hệ số wavelet trên ba băng tần cao của tập gồm 8 ảnh: Airplane.bmp, Beer.bmp, Elaine.bmp, House.bmp, Lena.bmp, Peppers.bmp, Sailboat.bmp, Tiffany.bmp (đã sử dụng trong 3.2.2.2) được các biểu đồ tương ứng theo hình 3.11.



Hình 3.11. Biểu đồ tần suất hệ số wavelet trên các băng tần cao của các ảnh gốc: a) Airplane.bmp, b) Beer.bmp, c) Elaine.bmp, d) House.bmp, e) Lena.bmp, f) Peppers.bmp, g) Sailboat.bmp, h) Tiffany.bmp

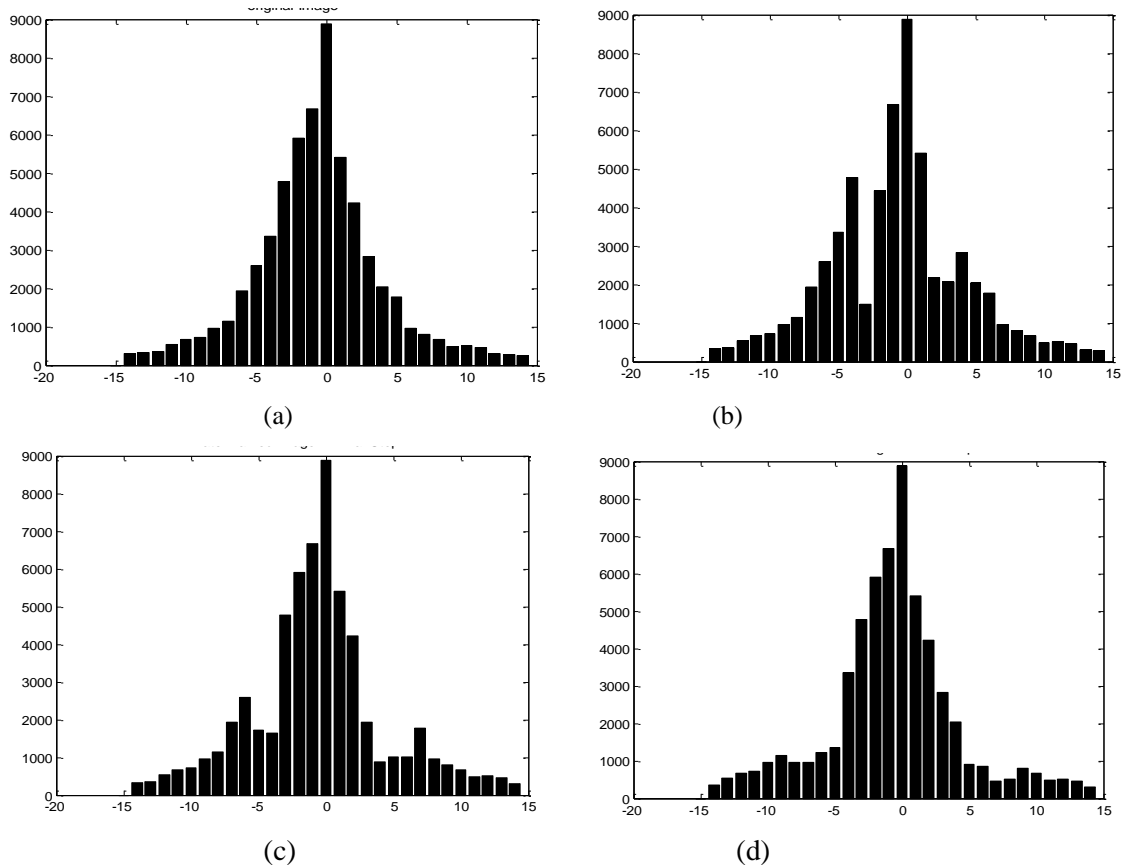
Tiếp theo chúng ta khảo sát chi tiết biểu đồ tần suất của ảnh Lena.bmp sau khi giấu thông tin là một ảnh Logo nhị phân kích cỡ 128x56 điểm ảnh (ứng với

7168 bit (hình 3.4. (b)) sử dụng kỹ thuật giấu IWH với các vị trí chọn  $T$  ban đầu khác nhau theo ba thử nghiệm sau:

Trong thử nghiệm thứ nhất, nhúng thông tin trên ba băng tần cao (HH, LH, HL) với vị trí bắt đầu là  $T = 2$ , sau khi giấu thông tin xong nhận được điểm dừng  $St = -2$ , lúc này biểu đồ tần suất của ảnh bị thay đổi như hình 3.12 (b).

Trong thử nghiệm thứ hai, vị trí khởi điểm chọn  $T = 4$ , nhận được điểm dừng  $St = 3$ . Trong trường hợp này biểu đồ thay đổi như hình 3.12 (c).

Trong thử nghiệm thứ ba, vị trí khởi điểm chọn  $T = 6$  và nhận được điểm dừng  $St = -5$ , lúc này biểu đồ thay đổi như hình 3.12 (d).



Hình 3.12. Biểu đồ tần suất hệ số wavelet trên các băng tần cao: (a) của ảnh Lena gốc và sau khi giấu tin với các vị trí chọn ban đầu: (b)  $T = 2$ , (c)  $T = 4$ , (d)  $T = 6$ .



So sánh sự khác biệt giữa biểu đồ tần suất các hệ số wavelet của ảnh gốc (hình 3.11) và ảnh có giấu tin với các điểm chọn ban đầu khác nhau T (hình 3.12), ta thấy trong một ảnh gốc điển hình thì:

$$h_0 > h_1 > h_2 > h_3 > \dots \text{ và } h_0 > h_{-1} > h_{-2} > h_{-3} > \dots$$

với  $h_i$  là số hệ số wavelet có giá trị bằng  $i$ .

Trong khi đó biểu đồ tần suất của ảnh sau khi giấu thông tin trong thử nghiệm thứ nhất ta thấy:

$$h_4 > h_3, h_3 \approx h_2, h_{-4} > h_{-3}, h_{-3} < h_{-2}$$

Trong thử nghiệm thứ hai:

$$h_5 \approx h_6, h_{-5} \approx h_{-4}, h_4 < h_3, h_4 < h_5,$$

Trong thử nghiệm thứ ba có:

$$h_7 \approx h_8, h_5 \approx h_6, h_{-7} \approx h_{-8}, h_{-5} \approx h_{-6}.$$

Vấn đề trên có thể giải thích dựa vào phân tích thí nghiệm thứ ba như sau: Phương pháp giấu tin IWH ban đầu dịch chuyển một phần cột tần suất với giá trị lớn hơn 6 (do  $T = 6, Z = T$ ) sang bên phải một đơn vị, tạo ra cột rỗng tại vị trí có hệ số wavelet bằng 7 ( $h_7 = 0$ ). Sau đó nhúng một phần thông tin vào  $h_6$  và  $h_7$  ta được  $h_6 \approx h_7$ . Vì thông tin chưa nhúng hết, do đó  $Z = 6$  chuyển thành  $Z = -6$ , ở đây thông tin còn lại được nhúng hết vào biểu đồ tại  $h_{-6}$  và  $h_{-7}$ , sau khi nhúng xong ta được  $h_{-6} \approx h_{-7}$ . Tuy nhiên thông tin cần nhúng vẫn còn nên  $Z = -6$  chuyển thành  $Z = 5$ ,  $h_6$  và  $h_7$  di chuyển thành  $h_7$  và  $h_8$ , thông tin được nhúng vào  $h_5$  và  $h_6$  nên  $h_5 \approx h_6$ . Tiếp tục  $Z = 5$  chuyển thành  $Z = -5$  (chưa nhúng hết thông tin),  $h_{-6}$  và  $h_{-7}$  di chuyển sang  $h_{-7}$  và  $h_{-8}$  để nhúng một phần thông tin, thông tin còn lại được nhúng vào một phần của  $h_{-5}$ , nó làm cho một phần của  $h_{-5}$  trở thành  $h_{-6}$  (do phần thông tin còn lại xấp xỉ bằng  $h_{-5}$  lên chúng ta thấy  $h_{-5} \approx h_{-6}$ ). Cuối cùng, quá trình nhúng tin kết thúc và đặt  $St=Z=-5$  (St: điểm dừng).

Từ các vấn đề phân tích ở trên, luận án xây dựng được thuật toán phát hiện ảnh có giấu tin trên các hệ số wavelet tổng quát dựa trên phương pháp ước lượng độ dài bit thông tin theo thuật toán 3.5.

### **Thuật toán 3.5 - Phát hiện ảnh stego\_IWH**

**Đầu vào :** Ảnh C cần kiểm tra

**Đầu ra:** Kết luận ảnh C có giấu tin bằng IWH hay không

**Bước 1.** Chuyển miền dữ liệu ảnh sang miền tần số wavelet giống như quá trình giấu tin IWH. Tính tần suất các hệ số wavelet ở ba băng tần HH, LH, HL được h.

**Bước 2.** Khởi tạo độ dài thông tin ước lượng  $L=0$ , quét toàn bộ các cột tần suất  $h_i$  với từng hệ số wavelet  $i$  ( $i \geq 0, i \leq \max$  (max là hệ số wavelet nguyên có giá trị lớn nhất của các băng tần cao)), nếu gặp giá trị đầu tiên  $(h_i + h_{i+1})/2 < h_{i+2}$ , dừng quét, đặt  $\text{Peak} = i$  là vị trí đầu tiên để ước lượng bit thông tin. Nếu không có hệ số nào thỏa mãn thực hiện chọn ngược lại cho các hệ số wavelet nhỏ hơn 0 ( $(h_{-i} + h_{-(i+1)})/2 < h_{-(i+2)}$ ) với tính toán tương tự tại bước 3, 4, 5 cho các hệ số âm. Trong cả hai trường hợp đều không thỏa mãn thuật toán dừng lại và  $L=0$ .

**Bước 3.** Nếu  $h_{\text{Peak}} \approx h_{\text{Peak}+1}$ ,  $L=L + h_{\text{Peak}} + h_{\text{Peak}+1}$ ; đặt  $\text{Peak} = -\text{Peak}$  và thực hiện tiếp bước 4. Ngược lại thực hiện bước 5.

**Bước 4.** Nếu  $h_{\text{Peak}} \approx h_{\text{Peak}+1}$ ,  $L=L + h_{\text{Peak}} + h_{\text{Peak}+1}$ ; đặt  $\text{Peak} = -\text{Peak} - 1$  và quay lại bước 2. Ngược lại thực hiện bước 5.

**Bước 5.** Nếu  $h_{\text{Peak}+1} < h_{\text{Peak}+2}$  và  $h_{\text{Peak}+1} < h_{\text{Peak}}$  thì  $L= L + 2 * h_{\text{Peak}+1}$ . Quá trình ước lượng kết thúc.

Áp dụng thuật toán cho ba thử nghiệm ở trên, chúng ta ước lượng được độ dài dữ liệu nhúng trong ảnh theo bảng 3.11

**Bảng 3.11. Kết quả thử nghiệm ước lượng trên ảnh Lena nhúng 7168 bit**

| Độ dài dữ liệu giấu | Ngưỡng chọn T | Điểm dừng | Độ dài ước lượng được bằng thuật toán 3.5 |
|---------------------|---------------|-----------|---|
| 7168                | 2             | -2        | 7231                                      |
| 7168                | 4             | 3         | 6998                                      |
| 7168                | 6             | -5        | 7177                                      |

### 3.3.3. Các kết quả thử nghiệm

#### 3.3.3.1. Thử nghiệm

*Tập ảnh thử nghiệm:* Tập ảnh thử nghiệm là tập ảnh  $\mathcal{C}_0$  gồm 2088 ảnh.

*Giấu tin:* Tập ảnh  $\mathcal{C}_0$  được giấu cùng một chuỗi thông tin có độ dài 6000 bit bằng kỹ thuật giấu IWH với ngưỡng  $T=4$  được tập  $\mathcal{S}_{IWH\_6000}$ .

*Phân loại ảnh:* Sử dụng kỹ thuật phát hiện ảnh có giấu tin bằng IWH cho hai tập ảnh  $\mathcal{C}_0$  và  $\mathcal{S}_{IWH\_6000}$  ta được bảng kết quả 3.12 (tương ứng với hình 3.13).

**Bảng 3.12. Bảng kết quả phân loại ảnh có giấu tin bằng IWH trên tập  $\mathcal{C}_0$  và  $\mathcal{S}_{IWH\_6000}$**

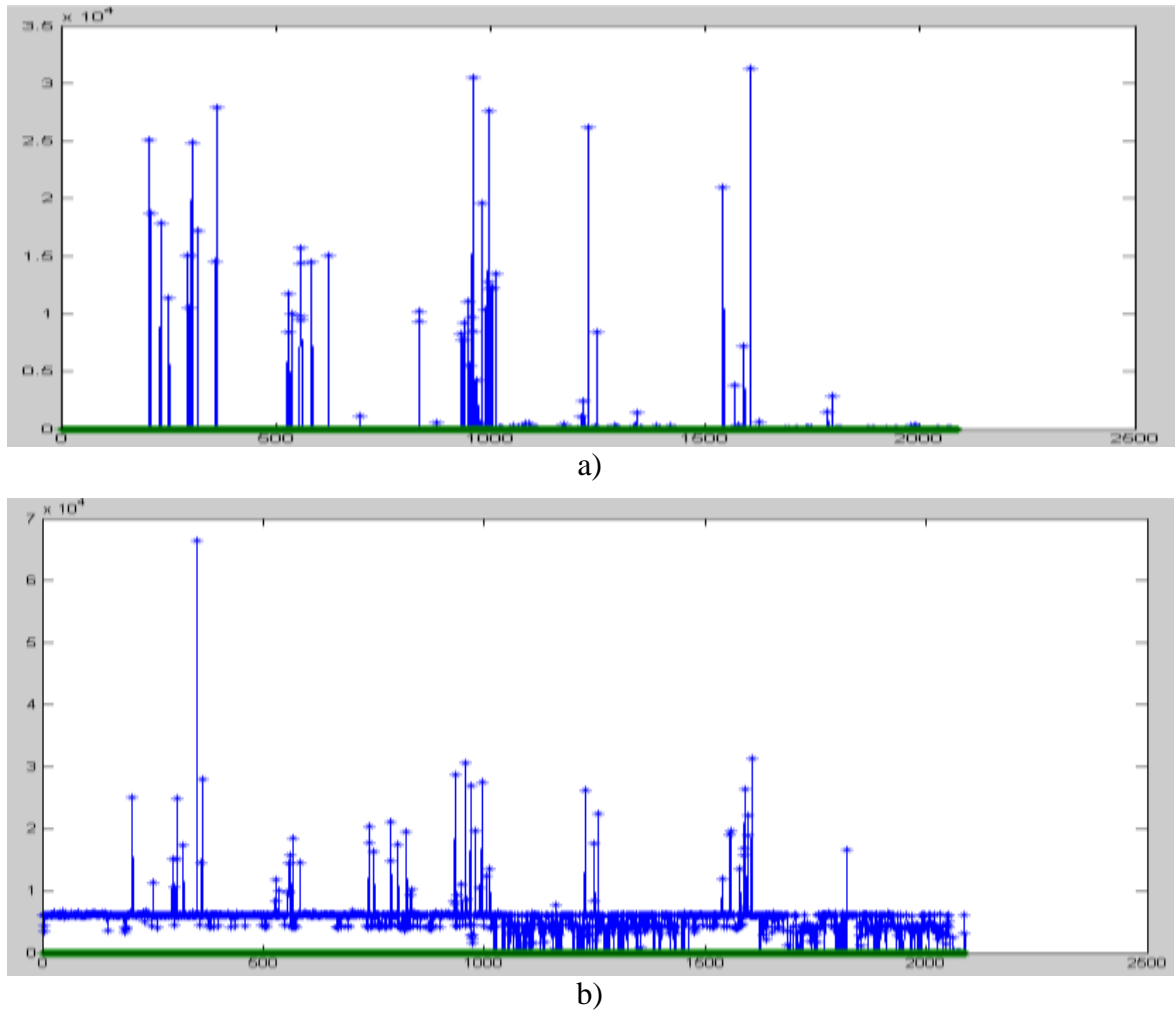
| Tập ảnh thử nghiệm        | Số ảnh phát hiện được với từng loại ảnh |                 |
|---------------------------|---|-----------------|
|                           | ảnh gốc                                 | ảnh có giấu tin |
| $\mathcal{C}_0$           | 1952                                    | 136             |
| $\mathcal{S}_{IWH\_6000}$ | 182                                     | 1906            |

Đánh giá kết quả trong bảng 3.12 theo độ đo P, R, F trên tập ảnh  $\mathcal{Y}$  gồm 4176 ảnh trong đó 2088 ảnh của tập  $\mathcal{C}_0$  và 2088 ảnh của tập  $\mathcal{S}_{IWH\_6000}$  ta được  $P = 0.91$ ,  $R = 0.93$ ,  $F = 0.92$ .

*Ước lượng thông tin giấu:* trong hai tập ảnh  $\mathcal{C}_0$  và  $\mathcal{S}_{IWH\_6000}$  ta được kết quả ước lượng trong bảng 3.13 ứng với hình 3.13.

**Bảng 3.13. Kết quả ước lượng thông tin giấu trên tập  $\mathcal{C}_0$  và  $\mathcal{S}_{IWH\_6000}$**

| Tập ảnh thử nghiệm        | Độ dài bit trung bình ước lượng | Độ lệch |
|---------------------------|---------------------------------|---------|
| $\mathcal{C}_0$           | 309                             | 2285    |
| $\mathcal{S}_{DIH\_6000}$ | 5301                            | 3165    |



Hình 3.13. Thử nghiệm ước lượng thông tin trên tập ảnh: a) tập  $\mathcal{C}_0$  và b) tập  $\mathcal{S}_{IWH\_6000}$

### 3.3.3.2. Nhận xét

Kỹ thuật giấu IWH có hình thức giấu giống kỹ thuật DIH chỉ khác là nó giấu trên các hệ số wavelet của băng tần con LH, HL và HH, do đó dựa vào phân tích biểu đồ tần suất trên các hệ số wavelet của các băng tần này, chúng ta có thể phát hiện ảnh có giấu tin sử dụng IWH với một số khẳng định sau:

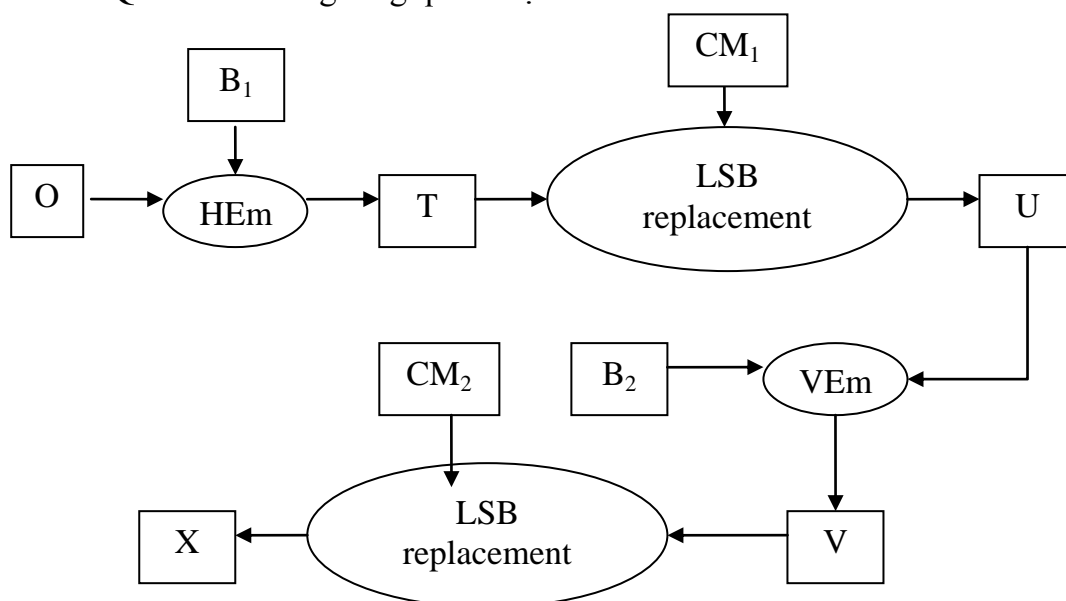
- Khả năng phát hiện ảnh có giấu tin với độ tin cậy cao. Sai số xảy phân loại ảnh gốc 0.09, sai số phân loại ảnh có giấu tin bằng 0.07.
- Có thể ước lượng xấp xỉ số bit thông tin giấu trong tập ảnh lớn với độ tin cậy là 0.09.

### 3.4. PHÁT HIỆN ẢNH CÓ GIẤU TIN SỬ DỤNG KỸ THUẬT GIẤU RVH

#### 3.4.1. Tóm lược kỹ thuật giấu tin RVH

Giấu tin hai pha ngang dọc hay còn gọi là kỹ thuật RVH (Reversible Vertical Horizontal Technique) do Mr. P. Mohan Kumar và Dr. K. L. Shunmuganathan đề xuất vào tháng 3 năm 2010 [45]. Kỹ thuật giấu này sử dụng chiến lược giấu nhiều lần nhằm nâng cao chất lượng ảnh và dung lượng giấu. Phương pháp giấu tin này sẽ nhúng một chuỗi bit thông tin vào các cặp giá trị điểm ảnh của ảnh  $O$  kích cỡ  $m \times n$  điểm ảnh theo thứ tự quét ảnh (từ trái sang phải, từ trên xuống dưới). Việc giấu tin sẽ chia ra làm 2 giai đoạn: Giai đoạn 1 gọi là giấu theo chiều ngang HEM (Horizontal embedding procedure) và giai đoạn 2 gọi là giấu theo chiều dọc VEM (Vertical embedding procedure).

Quá trình nhúng tổng quát được mô tả theo hình 3.14.



Hình 3.14. Mô hình tổng quát quá trình nhúng RVH

Chuỗi bit thông tin  $M$  với độ dài là  $L_M$  được chia làm 2 chuỗi con  $M_1$  và  $M_2$  với độ dài lần lượt là  $L_{M_1}$  và  $L_{M_2}$ . Tạo ra chuỗi bit thông tin  $B_1$  bằng cách ghép hai chuỗi là chuỗi bit  $M_1$  và chuỗi bit phụ  $A_1$ , nghĩa là  $B_1 = M_1 || A_1$ . Tương tự,  $B_2 = M_2 || A_2$ . Chuỗi  $A_1$  và  $A_2$  sẽ được giới thiệu ở phía sau.

Đầu tiên, các bit thông tin  $B_1$  sẽ nhúng theo chiều ngang vào  $O$  bằng thủ tục Hem (chi tiết bên dưới), cho ra ảnh  $T$ . Để có thể khôi phục các vị trí đã thay đổi

trong ảnh sau khi tách thông tin, nhóm tác giả sử dụng một bản đồ định vị HL là một ma trận hai chiều (kích thước  $m \times n/2$ ) giá trị nhị phân, ban đầu đều có giá trị 0, vị trí cặp điểm ảnh  $(x, y)$  nào trong ảnh O dùng để giấu tin sẽ được đánh dấu bằng 1 tương ứng trong ma trận định vị. Bản đồ định vị HL sẽ được nén lại thành  $CM_1$  bằng kỹ thuật nén JBIG2 [40] hoặc Carpenter [20], dữ liệu nén  $CM_1$  được nhúng vào T bằng kỹ thuật thay thế LSB tạo ra ảnh U.

Tiếp theo, chuỗi bit thông tin  $B_2$  được nhúng theo chiều dọc vào U bằng cách sử dụng thủ tục VEm (chi tiết bên dưới) để được ảnh kết quả V. Sử dụng bản đồ VL (tương tự như trong thủ tục giấu ngang Hem) kích cỡ  $n/2 \times m$  định vị vị trí các điểm ảnh có thể sử dụng giấu tin. Bản đồ VL được nén lại thành  $CM_2$  (sử dụng kỹ thuật nén JBIG2 [40] hoặc Carpenter [20]) được nhúng vào ảnh V bằng kỹ thuật thay thế LSB tạo ra ảnh stego X kích thước  $m \times n$ .

### ***Thủ tục nhúng ngang HEM***

Quét các điểm ảnh của ảnh O theo chiều ngang từng dòng một (từ trái qua phải từ trên xuống dưới) phân hoạch các điểm ảnh kề nhau  $x$  và  $y$  thành một cặp điểm ảnh  $(x, y)$  không trùng khớp. Nếu cặp  $(x, y)$  với  $y$  có giá trị lẻ thì cặp điểm ảnh  $(x, y)$  được định nghĩa là cặp điểm ảnh có thể nhúng ngang. Ngược lại, cặp  $(x, y)$  được định nghĩa không phải là cặp điểm ảnh có thể nhúng ngang. Gọi  $E_1$  là tập các cặp điểm ảnh có thể nhúng ngang của O có độ dài là  $LE_1$ . Những cặp điểm ảnh không thể nhúng ngang giữ nguyên giá trị. Mỗi bit thông tin  $b$  trong  $B_1$  được nhúng ngang vào mỗi cặp điểm ảnh  $(x, y) \in E_1$  bằng quy tắc nhúng ngang HR:

### ***Quy tắc nhúng ngang HR***

Với mỗi cặp điểm ảnh  $(x, y) \in E_1$ , chúng ta áp dụng các quy tắc sau:

HR<sub>1</sub>: nếu bit thông tin  $b = 1$ , thì cặp điểm ảnh đầu ra  $(x_0, y_0)$  được tính bằng  $(x_0, y_0) = (x, y)$ ,

HR<sub>2</sub>: nếu bit thông tin  $b = 0$ , thì cặp điểm ảnh đầu ra  $(x_0, y_0)$  được tính bằng  $(x_0, y_0) = (x, y - 1)$ .

Quy tắc nhúng ngang HR được lặp lại cho mỗi lần nhúng bit thông tin  $b$  của  $B_1$  vào ảnh  $O$  cho đến khi toàn bộ bit thông tin chuỗi  $B_1$  được nhúng hoàn toàn vào  $O$  để được ảnh đầu ra là  $T$ . Cần chú ý rằng quy tắc nhúng ngang HR không gây ra vấn đề tràn dưới và tràn trên. Do cặp điểm ảnh sau khi nhúng  $(x_0, y_0)$  luôn rơi vào khoảng phạm vi cho phép  $[0, 255]$ .

Chuỗi bit dữ liệu phụ  $A_1$  được thành lập như sau:

Bản đồ định vị HL sẽ được nén lại thành  $CM_1$  và có độ dài là  $LC_1$ . Lấy các bit LSB của điểm ảnh từ vị trí đầu ảnh đến vị trí  $LC_1$ , tập hợp của tất cả các bit đó là  $A_1$  sẽ được ghép vào sau  $B_1$  ( $B_1 = S_1 \parallel A_1$ ) và  $A_1$  được nhúng tiếp vào trong ảnh  $O$  bằng thủ tục HEM. Kết thúc ta được ảnh kết quả  $T$ .

### ***Thủ tục nhúng dọc VEm***

Ta duyệt từng cặp điểm ảnh  $(u, v)$  từ trên xuống dưới, từ trái qua phải của ảnh  $U$ . Nếu  $v$  là giá trị chẵn thì cặp điểm ảnh  $(u, v)$  được định nghĩa là cặp điểm ảnh có thể nhúng dọc. Ngược lại, cặp điểm ảnh  $(u, v)$  là cặp điểm ảnh không thể nhúng dọc. Tập các cặp điểm ảnh nhúng dọc của  $U$  là  $E_2$  có độ dài là  $LE_2$ . Những cặp điểm ảnh không thuộc tập  $E_2$  sẽ không bị thay đổi trong quá trình nhúng dọc. Mỗi bit thông tin  $b$  của  $B_2$  được nhúng dọc vào các cặp  $(u, v) \in E_2$  bằng cách sử dụng quy tắc nhúng dọc VR sau:

### ***Quy tắc nhúng dọc VR***

Tại mỗi cặp điểm ảnh nhúng dọc  $(u, v)$ , chúng ta áp dụng quy tắc nhúng sau:

VR<sub>1</sub>: nếu bit thông tin cần nhúng  $b = 0$ , thì cặp điểm ảnh kết quả  $(u_0, v_0)$  được tính bằng  $(u_0, v_0) = (u, v)$ .

VR<sub>2</sub>: nếu bit thông tin cần nhúng  $b = 1$ , thì cặp điểm ảnh kết quả  $(u_0, v_0)$  được tính bằng  $(u_0, v_0) = (u, v + 1)$ .

Quy tắc nhúng dọc VR được áp dụng lặp lại cho đến khi các bit thông tin của  $B_2$  được nhúng hết trong các cặp điểm ảnh  $(u, v)$  của  $E_2$ . Sau khi nhúng xong ta được ảnh  $V$ .

Cách tạo ra chuỗi bit dữ liệu phụ  $A_2$  như sau: Bản đồ định vị VL được xác định ngay khi có ảnh U. VL sẽ được nén lại (sử dụng kỹ thuật nén JBIG2 hoặc kỹ thuật nén của Carpenter) thành  $CM_2$  có độ dài là  $LC_2$ . Lấy các bit LSB của điểm ảnh từ vị trí đầu ảnh đến vị trí  $LC_2$ , tập hợp của tất cả các bit đó được chuỗi  $A_2$ , được ghép vào sau  $B_2$  ( $B_2 = S_2 \parallel A_2$ ) và  $B_2$  được nhúng tiếp vào trong ảnh U bằng thủ tục VEm. Kết thúc ta được ảnh kết quả là ảnh V.

### **3.4.2. Phương pháp phát hiện ảnh có giấu tin sử dụng kỹ thuật giấu RVH**

#### **3.4.2.1. Phân tích vấn đề giấu tin RVH**

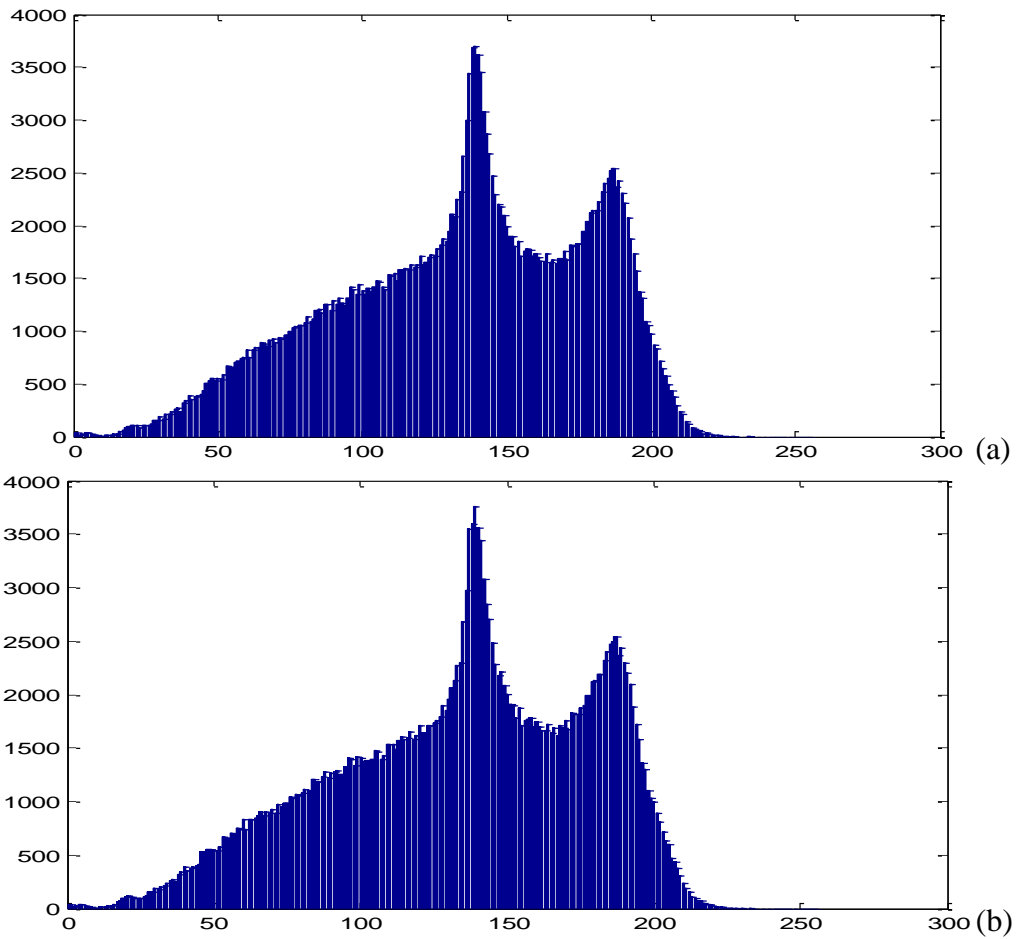
Kỹ thuật giấu RVH cũng là trường hợp riêng của kỹ thuật giấu LSB vì hai thủ tục giấu tin: thủ tục ngang HEm làm giảm giá trị  $y$  ( $y$  lẻ) của các cặp điểm ảnh  $(x, y) \in E_1$ , tức là LSB của  $y$  từ giá trị “1” chuyển sang “0”; thủ tục dọc VEm thực hiện ngược lại làm tăng giá trị  $v$  ( $v$  chẵn) của các cặp điểm ảnh  $(u, v) \in E_2$ , tức là LSB của  $v$  từ giá trị “0” chuyển sang “1”. Với hai thủ tục giấu tin ngang dọc này sẽ làm cân bằng lại LSB của các cặp giá trị ban đầu nghĩa là xác suất  $p(0)$  của bit “0” và  $P(1)$  của “1” trên miền LSB của ảnh là xấp xỉ bằng nhau hay  $P(0) \approx P(1)=0.5$  theo trạng thái tự nhiên ban đầu của ảnh. Để hiểu rõ kết luận này chúng ta hay xem khảo sát dưới đây trên ảnh gốc và ảnh sau khi giấu tin sử dụng kỹ thuật giấu RVH.

Giấu một chuỗi thông tin  $M$  với dung lượng lớn (tỉ lệ giấu 90% khả năng giấu lớn nhất của ảnh – số cặp điểm ảnh thuộc  $E_1$  và  $E_2$ ) vào ảnh cấp xám `cover_Baboon.bmp` kích cỡ 512 x 512 (xem hình 3.15), sử dụng kỹ thuật giấu RVH ta được ảnh `stego_Baboon.bmp`. Tính tần suất điểm ảnh của hai ảnh (`cover_Baboon.bmp` và `stego_Baboon.bmp`) ta được kết quả như hình 3.16.





Hình 3.15. Ảnh Baboon



Hình 3.16. Biểu đồ tần suất của: (a) ảnh cover\_Baboon, (b) ảnh stego\_Baboon

Từ hình 3.16 chúng ta thấy rất khó để phân biệt dấu hiệu khác biệt giữa hai ảnh trước và sau khi giấu vì theo nhận định của tác giả Kumar và cộng sự đề xuất

kỹ thuật giấu RVH dựa vào độ đo PSNR giữa ảnh gốc và ảnh giấu tin với lượng giấu lớn thì PSNR luôn luôn lớn hơn 54 dB, đây là độ đo lý tưởng trong xử lý ảnh.

Thực hiện kiểm tra bằng các phương pháp phát hiện tổng quát ảnh giấu LSB cho ảnh giấu RVH như sau: sử dụng tập ảnh  $\mathcal{C}_0$  (2088 ảnh) được giấu cùng lượng thông tin 7168 bit được tập kết quả  $\mathcal{S}_{RVH\_7168}$ . Sử dụng một số kỹ thuật phát hiện trong chương 2 và một số kỹ thuật của tác giả khác ta được kết quả phân loại trong bảng 3.14 và 3.15.

**Bảng 3.14. Kiểm tra ảnh stego trên tập  $\mathcal{S}_{RVH\_7168}$  bằng các kỹ thuật phát hiện tổng quát trên miền LSB**

|              | Phân loại ảnh bằng các kỹ thuật (số ảnh) |          |               |                 |           |
|--------------|--|----------|---------------|-----------------|-----------|
|              | “Độ lệch chuẩn”                          | $\chi^2$ | “Tỉ lệ xám 2” | $\chi_n^2$ [95] | LLRT [80] |
| ảnh gốc      | 468                                      | 509      | 588           | 598             | 302       |
| ảnh giấu tin | 132                                      | 91       | 12            | 2               | 298       |

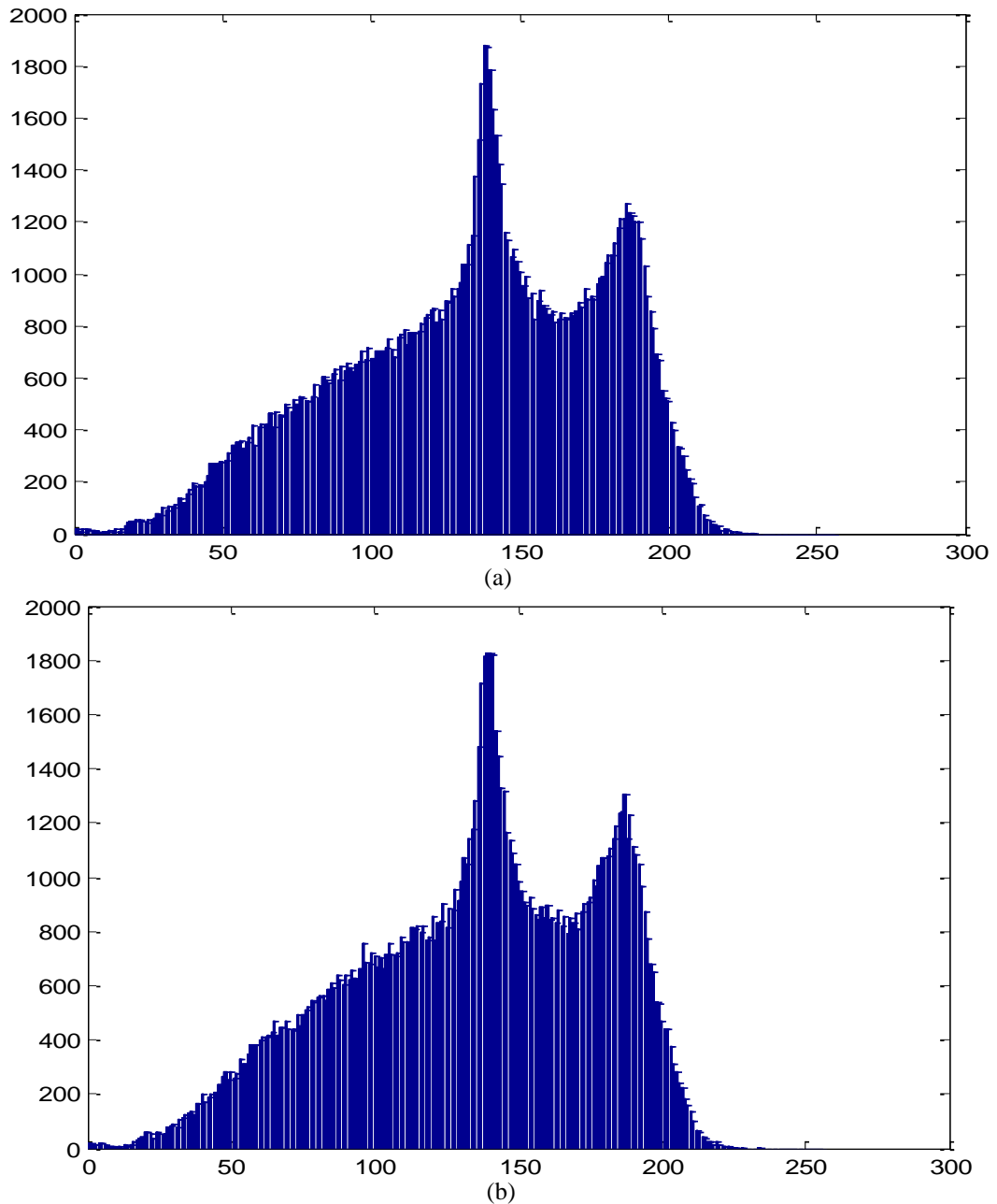
**Bảng 3.15. Ước lượng thông tin giấu cho tập  $\mathcal{S}_{RVH\_7168}$  bằng kỹ thuật RS, DI và “Trùng khớp”**

|  | RS [31]         | DI [102] | “trùng khớp” |
|--|-----------------|----------|--------------|
| <b>Kết quả ước lượng được trung bình</b> | R = 0.0015137 % | R = 12 % | R = 6 %      |

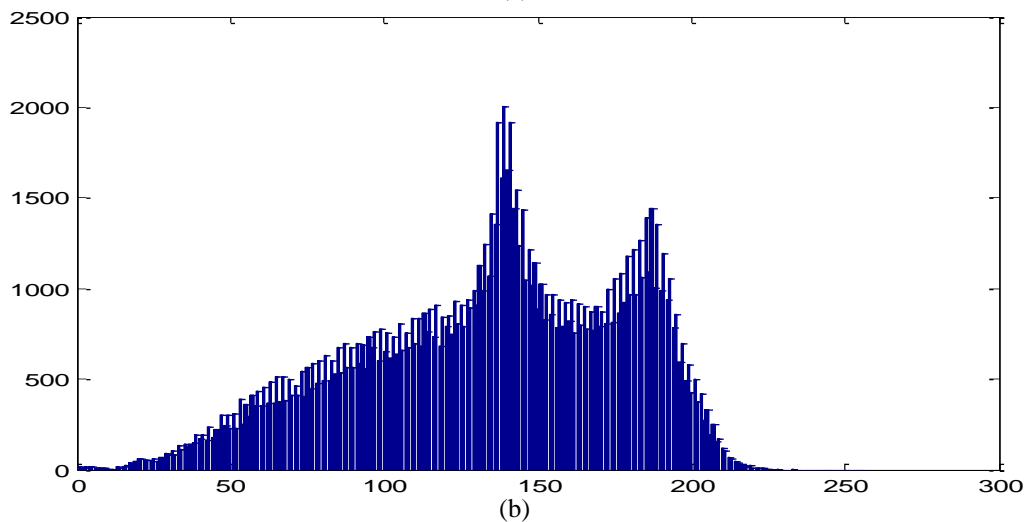
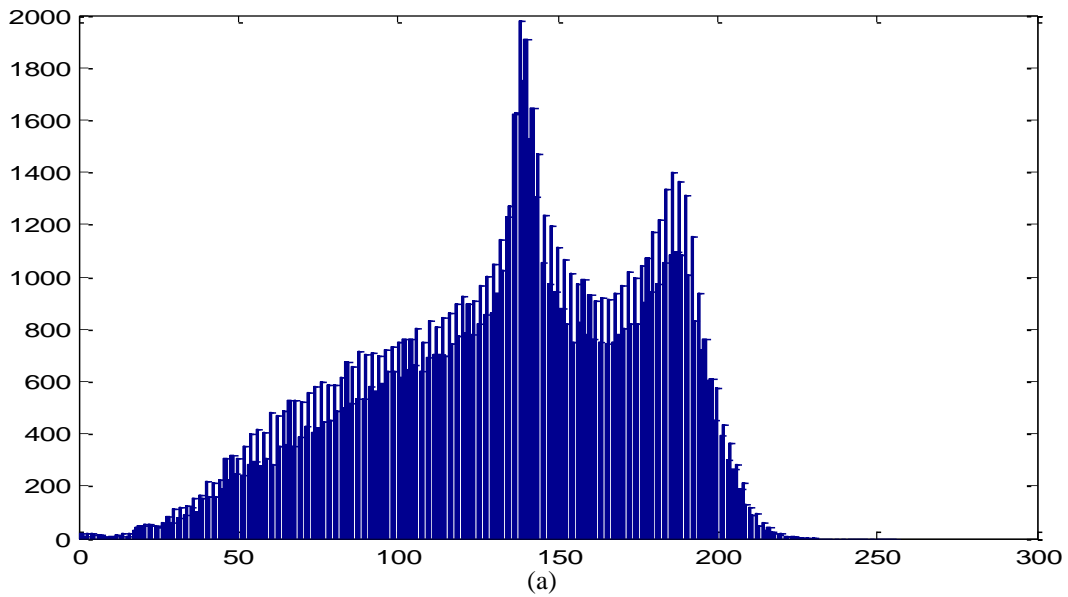
Từ bảng kiểm tra 3.14 và 3.15 chúng ta thấy với trường hợp giấu RVH nó có thể đưa ra kết quả phát hiện không chính xác cho các kỹ thuật phát hiện mù trên LSB. Vì vậy bằng phân tích tổng thể chúng ta khó có thể phát hiện ra ảnh có giấu tin sử dụng kỹ thuật giấu RVH, tuy nhiên bằng phương pháp phân tích từng phần chúng ta sẽ tìm ra dấu hiệu bất thường của kỹ thuật giấu RVH cho ảnh sau khi giấu tin. Trong 3.4.2.2 luận án đưa ra phương pháp phát hiện phù hợp cho kỹ thuật RVH và có thể ước lượng xấp xỉ thông tin giấu trong ảnh mà các kỹ thuật RS, DI và “Trùng khớp” chưa ước lượng được chính xác.

### 3.4.2.2. Phương pháp phát hiện và ước lượng thông tin

Để đưa ra phương pháp phát hiện cho kỹ thuật giấu RVH, chúng ta thực hiện một kiểm tra khác trên tần suất điểm ảnh bằng cách tách riêng biệt biểu đồ tần suất của các điểm ảnh trên các cột lẻ và cột chẵn của ảnh cover\_Baboon, ta được kết quả chỉ ra trên hình 3.17. Thực hiện tương tự trên ảnh stego\_Baboon, ta được kết quả chỉ ra trên hình 3.18.



Hình 3.17. Histogram trên các cột: (a) chẵn, (b) lẻ của ảnh cover\_Baboon. Bmp



Hình 3.18. Histogram trên các cột: (a) chẵn, (b) lẻ của ảnh *stego\_Baboon*. Bmp

Từ hình 3.17 và hình 3.18 chúng ta thấy với ảnh không giấu tin, biểu đồ tần suất trên các cột ở vị trí chẵn (hình 3.17 a) và trên các cột ở vị trí lẻ (hình 3.17 b) là rất giống nhau. Tuy nhiên với ảnh có giấu tin sử dụng kỹ thuật giấu RVH, biểu đồ tần suất trên các cột chẵn (hình 3.18 a) và trên các cột lẻ (hình 3.18 b), chúng ta dễ dàng nhận thấy dấu hiệu khác biệt giữa các cột tần suất của điểm ảnh chẵn và điểm ảnh lẻ so với ảnh không giấu tin. Điều này xảy ra do quá trình nhúng thông tin của kỹ thuật giấu RVH được giải thích chi tiết dưới đây.

Theo thủ tục nhúng ngang HEM, từ ảnh vào O, các điểm ảnh của ảnh O được nhóm theo hướng ngang thành các cặp  $(x, y)$ , các cặp này được phân hoạch vào hai tập  $E_1$  và  $\overline{E}_1$ , tập  $E_1$  bao gồm các cặp điểm ảnh  $(x, y)$  có thể nhúng ngang

(nghĩa là  $y$  có giá trị lẻ), trong khi  $\overline{E_1}$  là tập chứa các cặp  $(x, y)$  không thể nhúng ngang.

Chúng ta kiểm tra sự thay đổi tần suất LSB của ảnh  $O$  và ảnh  $T$  (ảnh đạt được sau khi nhúng  $B_1$ ). Để không mất tính tổng quát, đặt  $(x, y)$  và  $(\tilde{x}, \tilde{y})$  là các cặp điểm ảnh tương ứng trong ảnh  $O$  và ảnh  $T$ . Trong thủ tục nhúng ngang HEM, các cặp điểm ảnh  $(x, y) \in E_1$  (nghĩa là LSB của  $y$  có giá trị là “1”) được lựa chọn để nhúng bit thông tin. Ở đây chúng ta không kiểm tra sự thay đổi tần suất LSB của các điểm ảnh  $x$  trên các cột điểm ảnh ở vị trí chẵn của ma trận điểm ảnh, bởi vì chúng không bị thay đổi trong quá trình giấu bằng thủ tục ngang HEM.

Trong ảnh  $T$ , giá trị LSB của điểm ảnh  $\tilde{y}$  thay đổi thành “0” hoặc “1”, giá trị LSB của điểm ảnh  $y$  ban đầu là 1, sau khi giấu bit thông tin  $b$ , nếu  $b = 0$  ta được giá trị điểm ảnh mới của ảnh  $T$  là điểm ảnh  $\tilde{y}$  và LSB của nó bằng 0, nếu  $b = 1$  thì giá trị điểm ảnh mới  $\tilde{y}$  của ảnh  $T$  giữ nguyên (nghĩa là LSB của điểm ảnh  $\tilde{y}$  bằng 1). Trong ảnh tự nhiên thì xác suất của số bit “0” và số bit “1” trên các LSB là xấp xỉ bằng nhau và bằng 0.5. Vì vậy ảnh  $O$  là ảnh gốc nên xác suất của số bit “0” và số bit “1” là bằng 0.5. Sau khi giấu thông tin  $B_1$  sử dụng thủ tục nhúng ngang HEM xác suất của số bit “0” và số bit “1” của các LSB của điểm ảnh  $\tilde{y}$  là xấp xỉ bằng 0.5 (vì ta coi chuỗi bit  $B_1$  là các đại lượng phân bố ngẫu nhiên). Đối với các cặp điểm ảnh  $(x, y) \in \overline{E_1}$  (giá trị LSB của  $y$  bằng 0), sau khi giấu tin thì giá trị điểm ảnh  $\tilde{y}$  không thay đổi. Do đó xác suất của bit “0” và bit “1” trên LSB của điểm ảnh  $\tilde{y}$  lần lượt bằng 1 và 0.

Tiếp theo, bản đồ định vị đã bị nén  $CM_1$  ( $CM_1$  là một chuỗi nhị phân, với độ dài là  $LC_1$ ) được nhúng vào ảnh  $T$  bằng kỹ thuật thay thế LSB để được ảnh  $U$ . Điều này sẽ làm thay đổi một phần xác suất của bit 1 và bit 0 trên miền LSB của tất cả các cột điểm ảnh chẵn trong ảnh  $T$ . Giả sử các bit này được phân bố ngẫu nhiên, thì xác suất của bit 0 và bit 1 là  $P_{map1}(0) = P_{map1}(1)$ .

Dựa vào các vấn đề đưa ra ở trên, xác suất của bit “0” và bit “1” trên LSB của các điểm ảnh trên các cột chẵn trong ảnh  $U$  có thể tính toán. Giả sử xác suất của các cặp điểm ảnh thuộc tập  $E_1$  và xác suất của các cặp điểm ảnh thuộc  $\overline{E_1}$  lần lượt là

$P_{E1}$  và  $P_{\overline{E1}}$ . Sau khi giấu bản đồ định vị CM1,  $P_{E1}$  và  $P_{\overline{E1}}$  thay đổi thành  $P'_{E1}$  và  $P'_{\overline{E1}}$ . Đặt  $P_{R-H}$  là tỉ lệ nhúng (được định nghĩa bằng tỉ lệ số cặp  $(x, y)$  được sử dụng để giấu thông tin cho tổng số cặp trong ảnh O). Vậy xác suất của bit “0” và “1” trên LSB của các điểm ảnh ở vị trí cột chẵn trong ảnh U được tính bằng công thức sau:

$$P_{LSB_H}(b) = \begin{cases} P_{R-H} \times (0.5 \times P'_{E1} + P'_{\overline{E1}}) + P_{\overline{R-H}} \times 0.5 & \text{nếu } b = 0 \\ P_{R-H} \times (0.5 \times P'_{E1}) + P_{\overline{R-H}} \times 0.5 & \text{nếu } b = 1 \end{cases} \quad (3.17)$$

Đối với thủ tục nhúng dọc VEm, quét ảnh U theo chiều dọc với thứ tự quét từ trên xuống dưới, từ trái sang phải để nhóm các cặp điểm ảnh  $(u, v)$ , chúng ta phân loại ảnh vào hai tập  $E_2$  và  $\overline{E_2}$ , tập  $E_2$  gồm các cặp điểm ảnh có thể nhúng dọc, tập  $\overline{E_2}$  gồm các cặp điểm ảnh không thể nhúng dọc.

Đặt  $(u, v)$  và  $(\tilde{u}, \tilde{v})$  là các cặp điểm ảnh của ảnh U (trước khi sử dụng thủ tục VEm) và ảnh V (sau khi nhúng thông tin sử dụng VEm). Trong thủ tục VEm, chỉ các cặp điểm ảnh  $(u, v) \in E_2$ , nghĩa là LSB của  $v$  là bit 0, được dùng để nhúng thông tin. Sau khi giấu thông tin, giá trị LSB của  $\tilde{v}$  có thể là 0 hoặc 1. Vì vậy, xác suất của bit 0 và bit 1 của cặp  $(\tilde{u}, \tilde{v})$  bằng 0.5. Đối với các cặp  $(u, v) \in \overline{E_2}$  (giá trị LSB của  $v$  là 1) sau khi nhúng thông tin, giá trị  $\tilde{v}$  không thay đổi, trong trường hợp này xác suất của bit “0” và “1” lần lượt bằng 0 và 1.

Bản đồ định vị đã bị nén CM<sub>2</sub> được đánh dấu vào ảnh V bằng cách sử dụng kỹ thuật thay thế LSB để được ảnh X. Quá trình này sẽ làm thay đổi một phần xác suất các bit “0” và bit “1” trên LSB của các điểm ảnh ở vị trí hàng chẵn trong ảnh V. Giả sử các bit của CM<sub>2</sub> được phân bố ngẫu nhiên, thì xác suất của bit “0” và bit “1” là bằng nhau  $P_{map2}(0) = P_{map2}(1)$ .

Từ các phân tích đưa ra trong quá trình nhúng dọc, ta có thể tính xác suất của bit “0” và bit “1” trên LSB của các điểm ảnh ở vị trí hàng chẵn của ảnh X.

Đặt  $P_{E2}$  và  $P_{\overline{E2}}$  là xác suất của các cặp điểm ảnh thuộc  $E_2$  và  $\overline{E_2}$ , sau khi nhúng bản đồ định vị CM<sub>2</sub>,  $P_{E2}$  và  $P_{\overline{E2}}$  bị thay đổi thành  $P'_{E2}$  và  $P'_{\overline{E2}}$ .

Đặt  $P_{R-V}$  là tỉ lệ nhúng (bằng tỉ lệ số cặp điểm ảnh thực tế sử dụng để giấu tin chia cho tổng số cặp điểm ảnh của ảnh V). Xác suất của bit  $b = \{0,1\}$  trên LSB của ảnh X có thể tính theo công thức (3.18):

$$P_{\text{LSB-V}}(b) = \begin{cases} P_{\text{R-V}} \times (0.5 \times P'_{\text{E2}}) + P_{\text{R-V}} \times 0.5 & \text{nếu } b = 0 \\ P_{\text{R-V}} \times (0.5 \times P'_{\text{E2}} + P'_{\text{E2}}) + P_{\text{R-V}} \times 0.5 & \text{nếu } b = 1 \end{cases} \quad (3.18)$$

Đối với ảnh tự nhiên, LSB của ảnh được phân bố ngẫu nhiên, thì xác suất kỳ vọng của bit 0 và bit 1 trên LSB của các điểm ảnh ở vị trí hàng chẵn là như nhau, nghĩa là  $P_{\text{LSB}}(0) = P_{\text{LSB}}(1) = 0.5$ . Do đó xác suất  $P_{\text{E1}} = P_{\text{E1}} = 0.5$ . Sau khi bao phủ một phần LSB của ảnh T bằng bản đồ định vị nén CM<sub>1</sub> (sử dụng kỹ thuật thay thế LSB) với xác suất 0.05 (giả thiết), làm cho giá trị của  $P_{\text{E1}}$  và  $P_{\text{E1}}$  thay đổi thành  $P'_{\text{E1}} = 0.45$  và  $P'_{\text{E1}} = 0.55$ .

Ví dụ, xem xét ảnh Stego-Baboon.bmp từ ảnh Cover-Baboon.bmp, xác suất của các cặp điểm ảnh có thể nhúng thông tin (nghĩa là các cặp có thể sử dụng trong thủ tục nhúng ngang HEm) của ảnh đầu vào T là  $P'_{\text{E1}}$ , và 90% các cặp điểm ảnh trong E1 được sử dụng để nhúng thông tin, nghĩa là tỉ lệ nhúng của  $P_{\text{R-H}} = 0.45 \times 0.9 = 0.405$ .

Từ (3.17) chúng ta có:

$$P_{\text{LSB-H}}(0) = 0.405 \times (0.5 \times 0.45 + 0.55) + 0.595 \times 0.5 = 0.611375$$

$$P_{\text{LSB-H}}(1) = 0.405 \times (0.5 \times 0.45) + 0.595 \times 0.5 = 0.388625.$$

Tính xác suất của bit “0” và xác suất của bit “1” trên LSB của ảnh X. Chúng ta biết rằng xác suất của E<sub>2</sub> bằng xác suất của các LSB có giá trị “0” trên các hàng điểm ảnh chẵn, tức là  $P_{\text{E2}} = P_{\text{LSB}}(0)/2 + P_{\text{LSB-H}}(0)/2 = (0.5 + 0.611375)/2 = 0.5556875$  và  $P_{\text{E2}} = 0.4443125$ . Sau khi phủ một phần LSB của ảnh V bằng bản đồ định vị đã bị nén CM<sub>2</sub> với xác suất 0.05 (giả thiết), thì xác suất  $P_{\text{E2}}$  và  $P_{\text{E2}}$  thay đổi thành  $P'_{\text{E2}} = 0.5056875$  và  $P'_{\text{E2}} = 0.4943125$ .

Với tỉ lệ 90% các cặp điểm ảnh có thể nhúng được sử dụng để giấu thông tin, nghĩa là tỉ lệ nhúng của  $P_{\text{R-V}} = 0.5056875 \times 0.9 = 0.45511875$ . Vì vậy xác suất bit “0” và bit “1” trên LSB của ảnh đầu ra X theo (3.18), chúng ta được  $P_{\text{LSB-V}}(0) = 0.45511875 \times (0.5 \times 0.5056875) + 0.54488125 \times 0.5 \approx 0.3875$ , và  $P_{\text{LSB-V}}(1) = 0.61248$ .

Kiểm tra lại xác suất bit “0” và bit “1” của các LSB trên các cột chẵn:

$$P_{\text{LSB\_even\_column}}(0) = P_{\text{LSB\_H}}(0)/2 + P_{\text{LSB\_V}}(0)/2 = (0.611375 + 0.3875)/2 = 0.4994375,$$

$$P_{\text{LSB\_even\_column}}(1) = P_{\text{LSB\_H}}(1)/2 + P_{\text{LSB\_V}}(1)/2 = (0.388625 + 0.61248)/2 = 0.5005525.$$

Chúng ta thấy rằng xác suất của bit “0”,  $P_{\text{LSB\_even\_column}}(0)$ , và bit “1”,  $P_{\text{LSB\_even\_column}}(1)$ , là xấp xỉ bằng nhau, điều này nghĩa là sau khi hoàn thành thủ tục nhúng dọc VEm, nó làm cho giá trị của các xác suất này cân bằng nhau.

Tuy nhiên, xác suất của bit “0” và bit “1” của các LSB của các điểm ảnh trên cột lẻ của ảnh đầu ra X không xấp xỉ bằng nhau theo tính toán sau:

$$P_{\text{LSB\_odd\_column}}(0) = P_{\text{LSB\_org\_odd\_column}}(0)/2 + P_{\text{LSB\_V}}(0)/2 = (0.5 + 0.3875)/2 = 0.44375,$$

$$P_{\text{LSB\_odd\_column}}(1) = P_{\text{LSB\_org\_odd\_column}}(1)/2 + P_{\text{LSB\_V}}(1)/2 = (0.5 + 0.61248)/2 = 0.55624.$$

Trong đó  $P_{\text{LSB\_org\_odd\_column}}(0)$  và  $P_{\text{LSB\_org\_odd\_column}}(1)$  là xác suất của bit “0” và bit “1” của các LSB trên các cột lẻ của ảnh X.

Một nửa giá trị trên các cột này không bị thay đổi trong suốt quá trình của lược đồ RVH, vì vậy  $P_{\text{LSB\_org\_odd\_column}}(0)/2$  và  $P_{\text{LSB\_org\_odd\_column}}(1)/2$  đều xấp xỉ bằng 0.5/2. Sau sự thay đổi này sẽ làm cho xác suất bit “0” và bit “1” của các LSB trên các cột chẵn bị thay đổi theo.

Do đó, chúng ta có thể thấy sự khác biệt xảy ra của các bit “0” và bit “1” trong các cột lẻ và cột chẵn của ảnh có giấu tin sử dụng kỹ thuật RVH so với ảnh gốc.

Dựa vào sự thay đổi chênh lệch giữa xác suất của bit “0” và bit “1” theo các hàng chẵn trong ma trận dữ liệu ảnh ta có thể ước lượng sấp xỉ thông tin giấu trong ảnh theo thủ tục dọc VEm là  $L_H$  được tính theo biểu thức sau:

$$L_H = 2 * |P_{\text{LSB\_H}}(0) - P_{\text{LSB\_H}}(1)| * m/2 * n$$

Với m và n là kích thước của ảnh. Do một phần LSB của ảnh có độ dài  $L_{\text{CM2}}$  được sử dụng để nhúng bản đồ định vị đã được nén thì chúng ta đã phải sử dụng chuỗi  $A_2$  để lưu các LSB ban đầu của ảnh V và được nối vào chuỗi  $M_2$  của  $B_2$ . Vì vậy thực chất chuỗi số bit thông tin làm thay đổi  $|P_{\text{LSB\_H}}(0) - P_{\text{LSB\_H}}(1)|$  trong ảnh V chính là  $M_2$ . Do đó  $L_H$  là độ dài bit thông tin đã nhúng theo chiều dọc.



Mặt khác  $M = M_1 \parallel M_2$  và độ dài  $M_1$  bằng độ dài  $M_2$ , vì vậy độ dài bit thông tin đã giấu trong ảnh  $L$  có thể ước lượng biểu thức sau:

$$L = 2 * L_H = 4 * |P_{LSB\_H}(0) - P_{LSB\_H}(1)| * m/2 * n$$

Từ các vấn đề phân tích ở trên, luận án đưa ra định lý 3.8 để phân biệt và ước lượng thông tin của ảnh có giấu tin sử dụng kỹ thuật giấu RVH với một ảnh tự nhiên (ảnh gốc).

*Định lý 3.5 – Đặt  $P_{LSB}(0)$  và  $P_{LSB}(1)$  là xác suất bit “0” và bit “1” trên LSB của các cột điểm ảnh chẵn trong ảnh  $O$ . Khi đó ảnh  $O$  có giấu tin bằng RVH nếu:*

$$|P_{LSB}(0) - P_{LSB}(1)| > T \quad (3.19)$$

*Với  $T$  ( $0 \leq T \leq 1$ ) là ngưỡng để phân loại.*

*Lượng bit thông tin giấu trong ảnh được tính theo:*

$$L = |P_{LSB}(0) - P_{LSB}(1)| * 4 * m/2 * n \quad (3.20)$$

Chứng minh:

Dựa vào kỹ thuật giấu RVH ta thấy để phát hiện ảnh có giấu tin chúng ta chỉ cần xác định LSB trên các cột chẵn của ma trận dữ liệu điểm ảnh.

Với ảnh không giấu tin thì xác suất bit “0” và bit “1” trên miền LSB này là xấp xỉ bằng nhau ( $P(0)=P(1)=0.5$ ).

Sau khi giấu tin bằng RVH chúng ta xây dựng được biểu thức thay đổi xác suất bit “0” và bit “1” với pha giấu ngang là (3.17) và pha giấu dọc là (3.18).

Từ đó ta có thể thấy  $P_{LSB}(0)$ ,  $P_{LSB}(1)$  sẽ không còn xấp xỉ bằng nhau sau khi giấu tin sử dụng kỹ thuật giấu RVH. (3.21)

Dựa vào sự thay đổi chênh lệch giữa xác suất của bit “0” và bit “1” theo các hàng chẵn trong ma trận dữ liệu ảnh ta có thể ước lượng sấp xỉ thông tin giấu trong ảnh theo thủ tục dọc VEm là  $L_H$  được tính theo biểu thức sau:

$$L_H = 2 * |P_{LSB\_H}(0) - P_{LSB\_H}(1)| * m/2 * n$$

Với  $m$  và  $n$  là kích thước của ảnh. Do một phần LSB của ảnh có độ dài  $L_{CM2}$  được sử dụng để nhúng bản đồ định vị đã được nén thì chúng ta đã phải sử

dụng chuỗi  $A_2$  để lưu các LSB ban đầu của ảnh  $V$  và được nối vào chuỗi  $M_2$  của  $B_2$ . Vì vậy thực chất chuỗi số bit thông tin làm thay đổi  $|P_{LSB\_H}(0) - P_{LSB\_H}(1)|$  trong ảnh  $V$  chính là  $M_2$ . Do đó  $L_H$  là độ dài bit thông tin đã nhúng theo chiều dọc.

Mặt khác  $M = M_1 || M_2$  và độ dài  $M_1$  bằng độ dài  $M_2$ , vì vậy độ dài bit thông tin đã giấu trong ảnh  $L$  có thể ước lượng biểu thức sau:

$$L = 2 * L_H = 4 * |P_{LSB\_H}(0) - P_{LSB\_H}(1)| * m/2 * n \quad (3.22)$$

Từ (3.21) và (3.22) ta được điều phải chứng minh.

Áp dụng định lý 3.5 chúng ta có thuật toán 3.6 phát hiện ảnh có giấu tin sử dụng kỹ thuật giấu RVH dưới đây.

### **Thuật toán 3.6 – Phát hiện ảnh stego\_RVH**

**Đầu vào :** Một ảnh  $C$  bất kỳ

**Đầu ra:** Kiểm tra xem ảnh  $C$  có giấu tin bằng RVH hay không

**Bước 1.** Biểu diễn dữ liệu ảnh  $C$  dưới dạng ma trận hai chiều  $X$ .

**Bước 2.** Tính xác suất  $P(0)$  và  $P(1)$  của các bit “0” và bit “1” trên LSB của các cột chẵn của ma trận  $X$ .

**Bước 3.** Nếu  $P(0)$  và  $P(1)$  thỏa mãn (3.19) thì kết luận: Ảnh  $C$  là ảnh có giấu tin bằng kỹ thuật giấu RVH với lượng tin giấu được xác định dựa vào (3.20). Ngược lại, kết luận ảnh  $C$  không giấu tin bằng RVH.

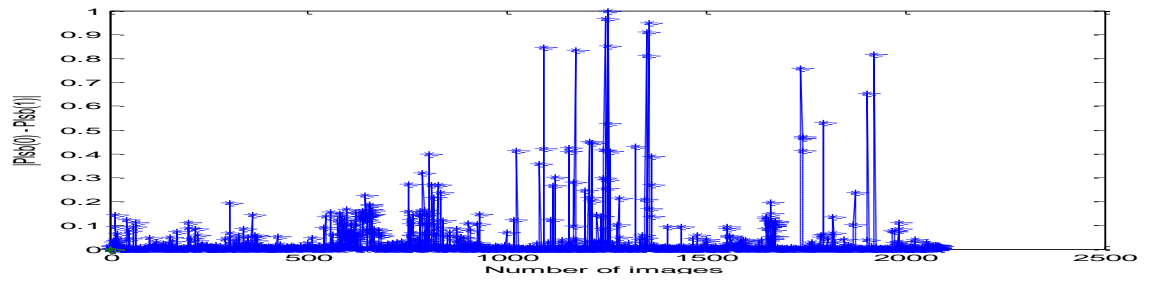
### **3.4.3. Các kết quả thử nghiệm**

#### **3.4.3.1. Thử nghiệm**

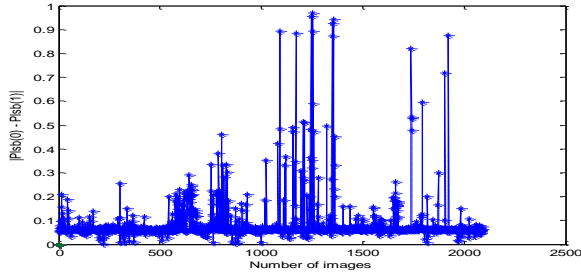
*Tập ảnh thử nghiệm:* là tập  $\mathcal{C}_0$  gồm 2088 ảnh.

*Giấu tin:* Sử dụng kỹ thuật giấu RVH để nhúng thông tin với lượng nhúng khác nhau, ứng với các tỉ lệ nhúng 25%, 50%, 75% và 100% khả năng nhúng có thể của ảnh được các tập tương ứng  $\mathcal{S}_{RVH\_R25}$ ,  $\mathcal{S}_{RVH\_R50}$ ,  $\mathcal{S}_{RVH\_R75}$ ,  $\mathcal{S}_{RVH\_R100}$ .

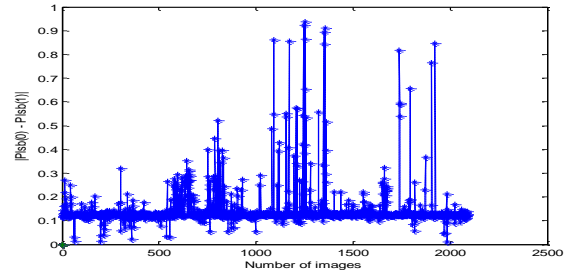
*Phân loại ảnh:* Kiểm tra sự thay đổi xác suất của các bit LSB “0” và “1” của các điểm ảnh trên các vị trí hàng chẵn của năm tập ảnh  $\mathcal{C}_0$ ,  $\mathcal{S}_{RVH\_R25}$ ,  $\mathcal{S}_{RVH\_R50}$ ,  $\mathcal{S}_{RVH\_R75}$ ,  $\mathcal{S}_{RVH\_R100}$  bằng (3.19), các kết quả đạt được chỉ ra trong hình 3.19.



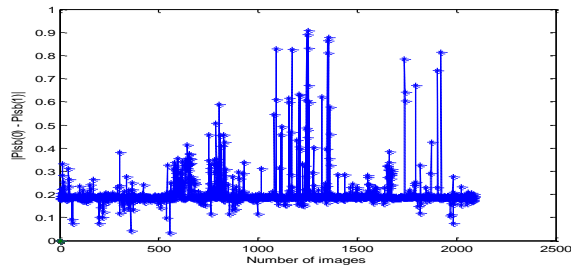
a)



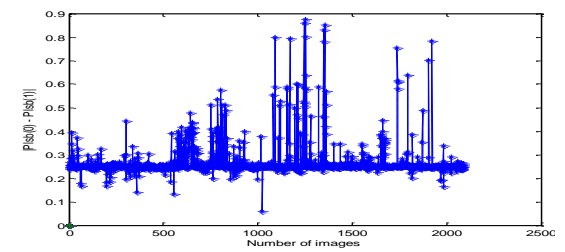
b)



c)



d)



e)

Hình 3.19. Sự phân bố của các giá trị  $|P_{LSB}(0) - P_{LSB}(1)|$  của các điểm ảnh trên các hàng chẵn trong tập: a)  $\mathcal{C}_0$ , b)  $\mathcal{S}_{RVH\_R25}$ , c)  $\mathcal{S}_{RVH\_R50}$ , d)  $\mathcal{S}_{RVH\_R75}$ , e)  $\mathcal{S}_{RVH\_R100}$

Ta cũng kiểm tra độ chính xác của phương pháp đề xuất cho tần công RVH với các tỉ lệ khác nhau và một số giá trị ngưỡng T để có thể đưa ra lựa chọn ngưỡng T hợp lý theo bảng 3.16.

**Bảng 3.16. Tỷ lệ phân loại ảnh (góc và giấu tin) với một số giá trị ngưỡng T**

| Tập ảnh<br>Threshold T | $C_0$ |          | $S_{RVH\_R25}$ |          | $S_{RVH\_R50}$ |          | $S_{RVH\_R75}$ |          | $S_{RVH\_R100}$ |          |
|------------------------|-------|----------|----------------|----------|----------------|----------|----------------|----------|-----------------|----------|
|                        | Góc   | Giấu tin | Góc            | Giấu tin | Góc            | Giấu tin | Góc            | Giấu tin | Góc             | Giấu tin |
| <b>0.01</b>            | 75.9  | 24.1     | 0.4            | 99.6     | 0              | 100      | 0              | 100      | 0               | 100      |
| <b>0.02</b>            | 84.8  | 15.2     | 0.7            | 99.3     | 0.1            | 99.9     | 0              | 100      | 0               | 100      |
| <b>0.03</b>            | 87.2  | 12.8     | 0.9            | 99.1     | 0.2            | 99.8     | 0              | 100      | 0               | 100      |
| <b>0.04</b>            | 88.9  | 11.1     | 2.3            | 97.7     | 0.4            | 99.6     | 0.04           | 99.96    | 0               | 100      |
| <b>0.05</b>            | 90.1  | 9.9      | 4.6            | 95.4     | 0.5            | 99.5     | 0.09           | 99.91    | 0               | 100      |

Từ bảng 3.16 cho thấy nếu chọn  $T=0.03$  có thể phân loại tốt đối với cả ảnh gốc và ảnh có giấu tin, nếu chọn  $T$  càng nhỏ thì phân loại không tốt cho ảnh gốc, còn  $T$  càng lớn thì phân loại không tốt cho ảnh giấu tin bằng RVH.

*Ước lượng thông tin:* Để đánh giá khả năng ước lượng thông tin, luận án sử dụng tập ảnh  $C_0$  giấu cùng chuỗi thông tin có độ dài 7500 bit được tập ảnh  $S_{RVH\_7500}$

**Bảng 3.17. Kết quả ước lượng thông tin giấu trên tập  $C_0$  và  $S_{RVH\_7500}$**

| Tập ảnh thử nghiệm | Độ dài bit trung bình ước lượng | Độ lệch |
|--------------------|---------------------------------|---------|
| $C_0$              | 536                             | 783     |
| $S_{RVH\_7168}$    | 7648                            | 2147    |

### 3.4.3.2. Nhận xét

Từ hình 3.19 có thể thấy hầu hết các giá trị của  $|P_{LSB}(0) - P_{LSB}(1)|$  tiệm cận 0 đối với các ảnh tự nhiên, trong khi với các tập  $S_{RVH\_R25}$ ,  $S_{RVH\_R50}$ ,  $S_{RVH\_R75}$ ,  $S_{RVH\_R100}$  thì  $|P_{LSB}(0) - P_{LSB}(1)|$  đạt giá trị lớn hơn 0 và đạt xấp xỉ 0.25 khi nhúng hết vào các cặp điểm ảnh có thể của ảnh.

Từ bảng 3.16, chúng ta thấy rằng giá trị ngưỡng hợp lý nhất với  $T = 0.03$ , có thể đưa ra kết quả chấp nhận được trong quá trình phát hiện ảnh stego sử dụng RVH. Bảng 3.17 cho thấy vấn đề ước lượng của thuật toán phát hiện ảnh có giấu tin bằng RVH là có thể tin cậy.

### **KẾT LUẬN CHƯƠNG 3**

Các phương pháp giấu thuận nghịch HKC, DIH, IWH, RVH là các trường hợp riêng của kỹ thuật giấu LSB, nó làm thay đổi rất ít trên LSB của miền không gian hay miền biến đổi. Do vậy nếu sử dụng một số phương pháp phát hiện mù bằng " $\chi_n^2$ ", LLRT, "độ lệch chuẩn", "tỉ lệ xám 1", "tỉ lệ xám 2", ... cho kết quả phân loại không cao, còn nếu dùng kỹ thuật phát hiện mù bằng phương pháp ước lượng có thể phát hiện ra ảnh nhưng không thể ước lượng chính xác bit thông tin đã giấu mà nó chỉ ước lượng được số bit tương ứng đã thay đổi trên LSB của ảnh.

Chương này đã đưa ra phương pháp phát hiện tối ưu cho từng kỹ thuật giấu đã biết (HKC, DIH, IWH, RVH) và có thể ước lượng xấp xỉ thông tin giấu trong ảnh sử dụng các kỹ thuật giấu này.

## KẾT LUẬN CHUNG

Phát hiện ảnh có giấu tin đang là bài toán cấp thiết hiện nay trong lĩnh vực an toàn bảo mật thông tin nói chung, lĩnh vực an ninh, chính trị và quốc phòng nói riêng. Phát hiện ảnh có giấu tin đòi hỏi phải được nghiên cứu một cách toàn diện từ các vấn đề của bài toán giấu tin trong ảnh.

### Các kết quả đạt được

Các phương pháp tiến hành nghiên cứu, lý thuyết và các kết quả thực nghiệm được trình bày trong hai chương chính là chương 2 và 3. Các kết quả chính của luận án là bốn kỹ thuật phát hiện mù cho ảnh có giấu tin trên LSB trên miền không gian, một kỹ thuật phát hiện mù cho ảnh có giấu tin trên LSB của miền tần số và bốn kỹ thuật phát hiện có ràng buộc cho ảnh có giấu tin sử dụng kỹ thuật giấu biết trước. Bám sát mục tiêu đề ra, các nội dung chính đạt được như sau:

1/. Đề xuất bốn kỹ thuật phát hiện mù cho ảnh có giấu tin trên LSB của miền không gian:

- Bằng phương pháp phân tích “độ lệch chuẩn”, đây là phương pháp được cho là phát hiện tốt hơn thống kê  $\chi^2$  với n bậc tự do của Westfeld và cộng sự [95]. Westfeld đưa ra phương pháp phát hiện bằng cách, với một ảnh số cấp xám 8-bit bất kỳ, để kiểm tra ảnh có giấu tin trên LSB hay không, thực hiện thống kê tần suất điểm ảnh vào vector  $C = \{c_i, i=0, \dots, 256\}$  với  $c_i$  là tần suất của điểm ảnh có giá trị  $i$  trong ảnh, họ thấy rằng với ảnh có giấu tin thì các cặp giá trị  $c_{2j}, c_{2j+1}$  ( $j=0, \dots, 127$ ) (gọi là cặp PoV – Pair of Values) trong vector  $C$  có giá trị xấp xỉ bằng nhau, trong khi với ảnh gốc thì điều này hiếm khi xảy ra. Do đó Westfeld sử dụng phương pháp thống kê  $\chi^2$  với  $n-1$  bậc tự do để phân loại ( $n$  được xác định từ số cặp PoV có giá trị khác 0). Phương pháp trên chỉ tỏ ra hiệu quả khi lượng thông điệp giấu là lớn và thứ tự giấu lần lượt theo chiều quét raster (từ trái sang phải, trên xuống), ngược lại thì không. Do đó để cải thiện vấn đề trên luận án đưa ra phương pháp phát hiện bằng cách thống kê tần suất điểm ảnh vào ma trận hai chiều  $S = \{s_{ij}, i=0, \dots, 26, j=0, \dots, 9\}$  với  $s_{ij}$  là tần suất của điểm ảnh có giá trị  $i*10+j$  trong ảnh. Khi đó sử dụng phân tích độ lệch chuẩn để phân loại theo ngưỡng  $t_0$  (dựa vào bảng “độ lệch chuẩn”), sẽ cho kết

- quả phát hiện tốt hơn trong trường hợp giấu với lượng thông tin nhỏ và được giấu rải rác trên các điểm ảnh (công bố trên công trình số 1).
- Bảng thống kê  $\chi^2$  một bậc tự do, có thể phát hiện có giấu tin tốt hơn “độ lệch chuẩn”. Từ quan sát trên một tập ảnh thực nghiệm (600 ảnh) với lượng thông điệp giấu lớn (từ 50% LSB của ảnh), chúng ta thấy rằng kỹ thuật giấu trên LSB sẽ làm thay đổi chủ yếu trên các điểm ảnh có tần suất lớn, do vậy nó làm cho giá trị tần suất điểm ảnh ở đây xấp xỉ bằng nhau hơn. Vì vậy cũng bằng phương pháp thống kê tần suất điểm ảnh vào ma trận hai chiều  $S = \{s_{ij}, i=0, \dots, 26, j=0, \dots, 9\}$  như trên, tìm hàng tại vị trí có  $s_{ij}$  lớn nhất của  $S$ , sau đó sử dụng thống kê  $\chi^2$  một bậc tự do cho cặp giá trị tổng chẵn và tổng lẻ tại hàng có giá trị lớn nhất đó để phân loại dựa vào ngưỡng  $t_0$  tìm được theo bảng thống kê  $\chi_n^2$  đã lập sẵn ứng với xác suất  $\alpha$  của sai số loại I cụ thể (công bố trên công trình số 3).
  - Bảng phân tích “tỉ lệ xám” giữa ảnh bất kỳ và ảnh dựng làm “mốc” cho kết quả phát hiện tốt hơn hai phương pháp trên cả về kết quả phân loại, thời gian thực hiện. Phương pháp phát hiện dựa này vào bỏ đề Neyman – Pearson, là bỏ đề phù hợp cho trường hợp với xác suất  $\alpha$  (sai số loại I) cho trước, chúng ta có thể cực tiểu hóa xác suất  $\beta$  (sai số loại II). Sullivan cũng đã áp dụng bỏ đề này trong [80] để phát hiện ảnh có giấu tin gọi là kỹ thuật LLRT, LLRT có thể phát hiện tốt với lượng thông điệp giấu nhỏ có tỉ lệ từ 5%. Tuy nhiên, phân loại chưa tốt trên tập ảnh gốc (ảnh làm mốc để phân loại) vì tác giả đưa ra phương pháp ước lượng xấp xỉ ảnh gốc từ một ảnh bất kỳ cần kiểm tra bằng phương pháp lọc thông thấp FIR [9]. Do vậy, luận án này đưa ra một trường hợp riêng của bỏ đề Neyman – Pearson với phương pháp ước lượng ảnh làm “mốc” khác, có thể phân loại tốt cho cả tập ảnh gốc và tập ảnh có giấu tin trên LSB (công bố trên công trình số 2).
  - Bằng phương pháp ước lượng thông tin giấu trên LSB của miền không gian ảnh sử dụng lý thuyết “trùng khớp”. Ban đầu ta ước lượng dựa trên một ảnh gốc  $C$  có trước, sau đó giấu một lượng thông tin vào ảnh  $C$  được ảnh  $S$ , ta thực hiện ước lượng thông tin trên ảnh  $S$  dựa vào ảnh  $C$  sẽ cho lượng thông tin xấp xỉ đã giấu trong ảnh. Tuy nhiên, trong thực tế chúng ta không có ảnh gốc, vì vậy ta phải xây dựng một ảnh để làm “mốc”, từ đó ta có thể ước lượng được thông tin giấu trong ảnh bất kỳ bằng lý thuyết trùng khớp đã xây dựng từ trường hợp có

ảnh gốc để so sánh. Dựa vào thực nghiệm cho thấy phương pháp ước lượng “trùng khớp” có thể ước lượng thông tin trên ảnh tương đương phương pháp ước lượng khác RS [31] và DI [102] nhưng tốt hơn về mặt thời gian thực hiện (công bố trên công trình số 4).

2/. Đề xuất một kỹ thuật phát hiện mù cho ảnh có giấu tin trên LSB của miền tần số cosine (wavelet) bằng:

- Phân tích tỉ lệ xám giữa ảnh bất kỳ và ảnh được dựng lên làm “mốc”. Phương pháp phát hiện này giống như “tỉ lệ xám” trên miền không gian, tức là cũng sử dụng bổ đề Neyman – Pearson nhưng thay vì thống kê trên tần suất điểm ảnh chúng ta thống kê trên tần suất của các hệ số cosine (wavelet) (công bố trên công trình số 2).

3/. Đề xuất bốn kỹ thuật phát hiện có ràng buộc cho ảnh có giấu tin sử dụng kỹ thuật giấu biết trước như:

- Kỹ thuật giấu HKC, là kỹ thuật giấu dựa trên dịch chuyển các cột tần suất điểm ảnh. Chính điều này làm tạo ra dấu hiệu không bình thường xung quanh cột tần suất có giá trị lớn nhất của biểu đồ tần suất điểm ảnh, vì vậy Wen-Chung Kuo và Yan – Hung Lin đưa ra phương pháp phát hiện [46] dựa vào mối quan hệ giữa cột tần suất lớn nhất Peak và bốn cột tần suất lân cận Peak để phát hiện ảnh có giấu tin sử dụng kỹ thuật HKC. Tuy nhiên kỹ thuật phát hiện của Kuo và Lin phát hiện có hiệu quả không cao trong trường hợp lượng bit thông tin giấu thấp, vì vậy luận án đưa ra phương pháp phát hiện cải tiến kỹ thuật của Kuo và Lin cho độ tin cậy cao hơn. Ngoài ra luận án còn xây dựng biểu thức phân loại tổng quát và đơn giản hơn của Kuo và Lin, dựa vào chính biểu thức mới này ta có thể ước lượng thông tin giấu trong ảnh sử dụng kỹ thuật giấu HKC (công bố trên công trình số 7).
- Kỹ thuật giấu DIH dựa vào các hệ số sai phân của ảnh. Kỹ thuật giấu DIH làm mất tính tự nhiên của biểu đồ tần suất các hệ số sai phân  $d_{ij}$ , biểu đồ này trong ảnh không giấu tin có phân bố theo biểu đồ Gausse [102], khi được giấu tin biểu đồ tần suất không còn phân bố đó nữa. Đây chính là yếu tố để luận án đưa ra phương pháp phát hiện ảnh có giấu tin sử dụng kỹ thuật giấu DIH (công bố trên công trình số 5).



- Kỹ thuật giấu IWH, là kỹ thuật giấu thuận nghịch dựa trên dịch chuyển các cột tần suất của biểu đồ tần suất hệ số wavelet của ba băng tần LL, LH, HL. Đây là một trường hợp riêng của kỹ thuật giấu LSB, tuy nhiên lượng thông điệp giấu với khả năng giấu cao nhất có thể vẫn rất thấp so với kỹ thuật giấu LSB thông thường, khi đó sử dụng kỹ thuật phát hiện mù trên LSB của miền tần số wavelet ( $\chi_n^2$ [95], “tỉ lệ xám” của luận án) thường cho kết quả phân loại không cao. Nhưng khi phân tích biểu đồ tần suất hệ số wavelet ta thấy được trạng thái không bình thường của biểu đồ khi giấu tin. Vì vậy luận án đưa ra phương pháp phát hiện tương ứng và có thể ước lượng xấp xỉ tỉ lệ bit thông tin giấu trong ảnh (công bố trên công trình số 5).
- Kỹ thuật giấu RVH (kỹ thuật giấu hai pha ngang dọc) sử dụng chiến lược giấu nhiều lần nhằm nâng cao chất lượng ảnh và dung lượng giấu. Thông tin cần giấu M được phân thành  $M_1$  và  $M_2$ . Quá trình giấu tin gồm hai pha chính: một pha giấu tin theo chiều ngang để giấu  $M_1$  và một pha giấu tin theo chiều dọc để giấu  $M_2$ . Đây là một trường hợp riêng của kỹ thuật giấu LSB, nhưng phương pháp giấu có thể tránh bị phát hiện bằng một số phương pháp phát hiện bằng thống kê như:  $\chi_1^2$ , “độ lệch chuẩn”, LLRT,... vì sử dụng giấu tin bằng hai pha sẽ tránh cân bằng các cặp PoV mà kỹ thuật giấu trên LSB thông thường gây ra. Do đó, để phát hiện luận án dựa vào phân tích tần suất bit “0” và bit “1” của LSB trên các cột điểm ảnh ở vị trí chẵn hoặc trên các hàng điểm ảnh ở vị trí lẻ của vector dữ liệu ảnh. Với ảnh không giấu tin thì xác suất của bit “0” và bit “1” xấp xỉ bằng nhau, tuy nhiên sau khi giấu thông điệp sử dụng RVH quy luật này bị phá vỡ. Luận án đã xây dựng được biểu thức tính xác suất các bit 0 và bit 1 sau mỗi pha giấu tin của RVH để từ đó có thể kiểm chứng được nhận định trên. Từ đó đưa ra thuật toán phát hiện và ước lượng xấp xỉ số bit thông tin cho ảnh có giấu tin sử dụng kỹ thuật giấu RVH (công bố trên công trình số 6).

Với một số phương pháp phát hiện mù trên miền LSB của ảnh, chúng ta không cần biết rõ phương pháp giấu là phương pháp nào, mà chỉ biết nó đã làm thay đổi tính tự nhiên trên LSB của miền không gian (miền tần số) của ảnh chưa giấu tin. Còn với các kỹ thuật phát hiện có ràng buộc cho ảnh có giấu tin sử dụng kỹ thuật giấu biết trước, luận án đã đưa ra hướng tiếp cận bằng cách phân tích biểu đồ tần suất của ảnh hay độ chênh lệch xác suất các bit “0” và bit “1” trên LSB của

miền không gian ảnh, từ đó có thể chỉ ra vấn đề không an toàn của kỹ thuật giấu bíêt trước đó.

### **Hướng phát triển của luận án**

Phát hiện ảnh có giấu tin là một vấn đề quan trọng trong lĩnh vực an toàn bảo mật thông tin đặc biệt trong lĩnh vực phân loại thông tin số trong môi trường truyền thông công cộng. Các kỹ thuật giấu tin mới trong ảnh liên tục được giới thiệu... Mỗi kỹ thuật giấu tin mới lại có nhiều ưu điểm và khó phát hiện hơn. Vấn đề phân tích và tìm ra các đặc trưng khác biệt giữa ảnh trước khi giấu thông điệp và sau khi giấu thông điệp là rất quan trọng đối với kỹ thuật phát hiện ảnh có giấu tin sử dụng kỹ thuật này. Theo hướng này, trong thời gian tới nghiên cứu sinh tiếp tục phát triển luận án với các nội dung sau:

- + Cải tiến thuật toán tăng độ chính xác của các kỹ thuật phát hiện đã có.
- + Đưa ra phương pháp trích chọn thông tin.
- + Tìm phương pháp phát hiện trên miền m\_LSBs
- + Phương pháp phát hiện giấu tin trong môi trường đa phương tiện khác như: Video, Audio ...

## DANH MỤC CÁC CÔNG TRÌNH CÔNG BỐ CỦA TÁC GIẢ

1. Hồ Thị Hương Thom, Hồ Văn Canh, Trịnh Nhật Tiến (2009), “Phát hiện ảnh có giấu tin bằng phương pháp phân tích độ lệch chuẩn”, *Kỷ yếu hội thảo Quốc gia Một số vấn đề chọn lọc của Công nghệ thông tin và Truyền thông lần thứ XI*, Huế, tr. 284-291.
2. Ho Thi Huong Thom, Ho Van Canh, Trinh Nhat Tien (2009), “Novel Algorithms to Steganalysis of Uncompressed and Compressed Images”, *Proceedings of KSE 2009 on Knowledge and Systems Engineering, College of Technology, IEEE Computer Society, Vietnam National University, Ha Noi*, pp. 87-92.
3. Ho Thi Huong Thom, Canh Ho Van, Tien Trinh Nhat (2009), “Statistical Methods to Steganalysis of Color or Grayscale Images”, *Proceedings of IEEE-RIVF 2009 on Doctoral Symposium, Da Nang University of Technology*, pp. 1-5.
4. Hồ Thị Hương Thom, Hồ Văn Canh, Trịnh Nhật Tiến (2010), “Ước lượng xấp xỉ thông điệp giấu trên miền LSB của ảnh”, *Kỷ yếu hội thảo Quốc gia Một số vấn đề chọn lọc của Công nghệ thông tin và Truyền thông lần thứ XII*, Đồng Nai, tr. 488 – 495.
5. Ho Thi Huong Thom, Ho Van Canh, Trinh Nhat Tien (2009), “Steganalysis to Reversible Data Hiding”, *Proceedings of FGIT 2009 (the Future Generation Information Technology Conference) on Database Theory and Application, Springer-Verlag, Jeju Island, Korea*, pp. 1- 6.
6. Thom Ho Thi Huong, Canh Ho Van, Tien Trinh Nhat (2010), “Steganalysis of Reversible Vertical Horizontal Data Hiding Technique”, *International Journal of Computer Science and Information Security (IJCSIS)*, Vol. 8 (6), pp. 7-12.
7. Hồ Thị Hương Thom, Hồ Văn Canh, Trịnh Nhật Tiến (2010), “Phát hiện ảnh giấu tin sử dụng kỹ thuật giấu thuận nghịch dựa trên dịch chuyển Histogram”, *Tạp chí Khoa học ĐHQGHN, Khoa học Tự nhiên & Công nghệ*, tập 26 (4), tr. 261-267.

## TÀI LIỆU THAM KHẢO

### Tiếng Việt

- [1]. Phan Đình Diệu (2002), *Lý thuyết mật mã và an toàn thông tin*, NXB Đại học Quốc gia Hà Nội.
- [2]. Dương Anh Đức, Dương Minh Đức (2004), “Nâng cao hiệu quả kỹ thuật ẩn thông tin trong ảnh số”, *Kỷ yếu hội thảo Quốc gia - Một số vấn đề chọn lọc của Công nghệ thông tin và Truyền thông lần thứ VII*, Đà Nẵng, tr. 100 - 107.
- [3]. Nguyễn Xuân Huy, Trần Quốc Dũng (2003), “Một thuật toán thủy vân số trên miền biến đổi Cosine rời rạc”, *Kỷ yếu hội thảo Quốc gia - Một số vấn đề chọn lọc của Công nghệ thông tin và Truyền thông lần thứ VI*, Đại học Thái Nguyên.
- [4]. Nguyễn Xuân Huy, Bùi Thế Hồng, Trần Quốc Dũng (2004), “Kỹ thuật thủy vân số trong ứng dụng phát hiện xuyên tạc ảnh”, *Kỷ yếu hội thảo Quốc gia - Một số vấn đề chọn lọc của Công nghệ thông tin và Truyền thông lần thứ VII*, Đại học Đà Nẵng, tr. 183 – 187.
- [5]. Bùi Thế Hồng, Nguyễn Văn Tảo (2006), “Kỹ thuật thủy vân sử dụng phép biến đổi sóng nhỏ rời rạc và ma trận số giả ngẫu nhiên”, *Hội nghị Khoa học kỷ niệm 30 năm Viện Công nghệ thông tin*.
- [6]. Trần Hồng Ngọc, Trương Thị Mỹ Trang (2004), “Các kỹ thuật giấu tin dựa trên phép biến đổi wavelet và ứng dụng”, *Kỷ yếu hội thảo Quốc gia - Một số vấn đề chọn lọc của Công nghệ thông tin và Truyền thông lần thứ VII*, Đại học Đà Nẵng, tr. 183 – 187.
- [7]. Nguyễn Văn Tảo, Bùi Thế Hồng (2006), “Nâng cao chất lượng ảnh trong kỹ thuật thủy vân sử dụng miền tần số giữa của phép biến đổi DCT”, *Tạp chí Tin học và Điều khiển học*, tập 4.
- [8]. Hồ Thị Hương Thơm, Hồ Văn Canh, Trịnh Nhật Tiến (2009), “Phát hiện ảnh có giấu tin bằng phương pháp phân tích độ lệch chuẩn”, *Kỷ yếu hội thảo Quốc gia - Một số vấn đề chọn lọc của Công nghệ thông tin và Truyền thông, lần thứ XI*, Huế, tr. 284 - 291.

- [9]. Hồ Thị Hương Thơm, Hồ Văn Canh, Trịnh Nhật Tiến (2010), “Ước lượng xấp xỉ thông điệp giấu trên miền LSB của ảnh”, *Kỷ yếu hội thảo Quốc gia - Một số vấn đề chọn lọc của Công nghệ thông tin và Truyền thông, lần thứ XII*, Đồng Nai, tr. 488 – 495.
- [10]. Hồ Thị Hương Thơm, Hồ Văn Canh, Trịnh Nhật Tiến (2010), “Phát hiện ảnh giấu tin sử dụng kỹ thuật giấu thuận nghịch dựa trên dịch chuyển histogram”, *Tạp chí Khoa học ĐHQGHN, Khoa học Tự nhiên & Công nghệ*, tập 26 (4), tr. 261-267.
- [11]. Nguyễn Quốc Trung (2001), *Xử lý tín hiệu và lọc số*, Nhà xuất bản Khoa học và kỹ thuật.

### **Tiếng Anh**

- [12]. I. Avcibas, N.Memon, and B. Sankur (2002), “Image steganalysis with binary similarity measures”, *In Processing of ICIP 2002*.
- [13]. Mohammad Awrangjeb (2003), “An Overview of Reversible Data Hiding”, *ICCIT 2003*, 19-21 Dec, Jahangirnagar University, Bangladesh, pp. 75-79.
- [14]. L. Bin, F. Yanmei, H. Jiwu, (2008), “Steganalysis of Multiple-Base Notational System Steganography”, *IEEE Signal Processing Letters*, vol. 15, pp. 493 - 496.
- [15]. C. Cachin (1998), “An information – theoretic model for steganography”, *In D. Aucsmith, editor, Information Hiding, 2<sup>nd</sup> International Workshop*, volume 1525 of LNCS, Springer – Verlag, New York, pp. 306 – 318.
- [16]. C.K. Chan, L.M. Cheng (2001), “Improved hiding data in images by optimal moderately-significant-bit replacement”, *IEEE Electronics Letters*, Vol. 37 (16), pp. 1017–1018.
- [17]. C.K. Chan, L.M. Cheng (2004), “Hiding data in images by simple LSB substitution”, *Pattern Recognition* 37, pp. 469–474.
- [18]. R. Chandramouli, M. Kharrazi and N. Memon (2004), “Image Steganography and Steganalysis: Concepts and Practice”, *international workshop on digital watermarking*, No. 2, COREE, REPUBLIQUE DE , vol. 2939, pp. 35-49.

- [19]. C.C. Chang, J.Y. Hsiao, C.S. Chan (2003), “Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy”, *Pattern Recognition* 36, pp. 1583–1595.
- [20]. Carpenter, B. (2002), “Compression via Arithmetic Coding”, <http://www.colloquial.com/ArithmeticCoding/>
- [21]. M.U. Celik, G. Sharma, A.M. Tekalp., and E. Saber (2002), “Reversible Data Hiding”, *In Proc. of International Conference on Image Processing*, Rochester, NY, USA, Vol. 2, pp. 157-160.
- [22]. Abbas Cheddad (2009), *Steganoflage: A New Image Steganography Algorithm*, Ph. D Thesis, University of Ulster, (<http://www.infm.ulst.ac.uk/~abbasc/Research.php>).
- [23]. B. Chen and G. Wornell (2001), “Quantization index modulation: A class of provably good methods for digital watermarking and information embedding”, *IEEE Trans. Info. Theory*, Vol. 47 (4), pp. 1423-1443.
- [24]. Yeh-Shun Chen, Ran-Zan Wang, Yeuan-Kuen Lee, Shih-Yu Huang (2008), “Steganalysis of reversible contrast mapping water marking”, *Proceedings of the world congress on Engineering 2008*, Vol I, WCE2008, London, U.K., pp. 555-557.
- [25]. D. Coltuc and J. M. Chassery (2007), “Very fast watermarking by reversible contrast mapping”, *IEEE Signal Processing Lett.*, vol. 14 (4), pp. 255– 258.
- [26]. J. K I. Cox, J. Kilian, T. Leighton, and T. Shamoan (1997), “Secure spread spectrum watermarking for multimedia”, *IEEE Trans. on Image Processing*, 6(12):1673–1687.
- [27]. Ingemar Cox, Jeffrey Bloom, Matthew Miller, Ton Kalker, Jessica Fridrich (2008), *Digital Watermarking and Steganography*, Second Edition, Morgan Kaufmann Press, USA.
- [28]. O. Dabeer, K. Sullivan, U. Madow, S. Chandrasekaran and B. S. Manjunath (2003), “Detection of hiding in the least significant bit”, *In Proc. Conference on Information Sciences and Systems (CISS)*.
- [29]. O. Dabeer, K. Sullivan, U. Madhow, S. Chandrasekaran and B.S. Manjunath (2004), “Detection of Hiding in the Least Significant Bit”, *In IEEE*

*Transactions on Signal Processing, Supplement on Secure Media I*, vol. 52, no. 10, pp. 3046–3058.

- [30]. S. Dumitrescu, X. Wu, and Z. Wang (2003), “Detection of LSB steganography via sample pair analysis”, *IEEE Trans. On Signal Processing* 2003, 51(7), pp. 1995-2007.
- [31]. Fridrich, J., Goljan, M., and Du, R. (2001), “Reliable Detection of LSB Steganography in Grayscale and Color Images”, *Proc. of ACM: Special Session on Multimedia Security and Watermarking*, Ottawa, Canada, pp. 27–30.
- [32]. Jessica Fridrich (2009), *Steganography in digital media: principles, algorithms, and applications*, Cambridge University Press.
- [33]. Jessica Fridrich, Miroslav Goljan, Dorin Hogeia (2006), “Steganalysis of JPEG Images: Breaking the F5 Algorithm”, *Pattern Recognition, ICPR 2006 18<sup>th</sup> International Conference*, Volume 2, pp. 267 – 270.
- [34]. J. Fridrich, M. Goljan, and D. Soukal (2003), “Higher-order statistical steganalysis of palette images”, in *Security and Watermarking of Multimedia Contents, Proc. SPIE 5020*, pp. 178–190.
- [35]. J. Fridrich, M. Goljan, and D. Rui (2002), “Lossless Data Embedding for all Image Formats”, In *Proc. SPIE Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents*, San Jose, California, USA, Vol. 4675, pp. 572-583.
- [36]. J. Fridrich, M. Goljan and D. Hogeia (2002), “Attacking the OutGuess”, *Proc. of the ACM Workshop on Multimedia and Security 2002*, Juan-les-Pins, France.
- [37]. Caxton Foster (1982), *Cryptanalysis for Microcomputers*, Rochelle Park, NJ, Hayden Book Co.
- [38]. S. P. Hivrle, S. D. Sawarkar, Vijay Bhosale, and Seema Koregaonkar (2008), “Statistical Method for Hiding Detection in LSB of Digital Images: An Overview”, *Proceedings of World Academy of Science, Engineering and Technology*, Volume 32, ISSN 2070 – 3740, pp. 658 – 661.

- [39]. C. W. Honsinger, P. Jones, M. Rabbani, and J. C. Stoffel (1999), “Lossless recovery of an original image containing embedded data”, *US Patent application*, Docket no: 77102/E-D.
- [40]. P.G. Howard, F. Kossentini, B. Martins, S. Forchhammer, W. J. Rucklidge (1998), “The emerging JBIG2 standard”, *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 8 (7), pp. 838-848.
- [41]. J.H. Hwang, J. W. Kim, and J. U. Choi (2006), “A Reversible Watermarking Based on Histogram Shifting”, *IWDW 2006*, pp. 384-361.
- [42]. Takayuki Ishida, Kazumi Yamawaki, Hideki Noda, Michiharu (2009), “Performance improvement of JPEG2000 steganography using QIM”, *Journal of Communication and Computer*, Volume 6 (1), USA.
- [43]. A. K. Jain (1989), *Fundamentals of Digital Image Processing*, Prentice – Hall.
- [44]. Makhoul, John; Francis Kubala; Richard Schwartz; Ralph Weischedel (1999), “Performance measures for information extraction”, *Proceedings of DARPA Broadcast News Workshop*, Herndon, VA.
- [45]. P. M. Kumar, K. L. Shunmuganathan (2010), “A reversible high embedding capacity data hiding technique for hiding secret data in images”, *International Journal of Computer Science and Information Security (IJCSIS)*, Vol.7 (3), pp. 109-115.
- [46]. Wen-Chung Kuo, Yan-Hung Lin (2008), “On the Security of Reversible Data Hiding Based-on Histogram Shift”, *ICICIC 2008*, pp. 174-177.
- [47]. Lehmann E. (1959), *Testing Statistical Hypothesis*, John Wiley, New York.
- [48]. Chih-Chiang Leea, Hsien-ChuWub, Chwei-Shyong Tsaic, Yen-Ping Chu, (2008), “Adaptive lossless steganographic schemewith centralized difference expansion”, *Pattern Recognition 41*, pp. 2097 – 2106.
- [49]. Sang-Kwang Lee, Young-Ho Suh, and Yo-Sung Ho (2004), “Lossless Data Hiding Based on Histogram Modification of Difference Images”, *Advances in Multimedia Information Processing - PCM 2004*, pp. 340-347.



- [50]. Xiaolong Li, Bin Yang, Daofang Cheng and Tieyong Zeng (2009), “A Generalization of LSB Matching”, *IEEE signal processing letters*, Vol. 16 (2), pp. 69 – 72.
- [51]. W.N. Lie, L.C. Chang (1999), “Data hiding in images with adaptive numbers of least significant bits based on the human visual system”, in: *Proceedings of IEEE International Conference on Image Processing*, Taipei, Taiwan, vol. 1, pp. 286–290.
- [52]. Chia-Chen Lin, Wei-Liang Tai, Chin-Chen Chang (2008), “Multilevel reversible data hiding based on histogram modification of difference images”, *Pattern Recognition 41*, Science Direct Journal, pp. 3582-3591.
- [53]. Ching-Chiuan Lin, Nien-Lin Hsueh (2008), “A lossless data hiding scheme based on three-pixel block differences”, *Pattern Recognition 41*, pp. 1415 – 1425.
- [54]. S. H. Liu, T. H. Chen, H. X. Yao and W. Gao (2004), “A variable depth LSB data hiding technique in images”, *Machine Learning and Cybernetics 2004*, pp. 3990-3994.
- [55]. Z. M. Lu, J. S. Pan, and S. H. Sun (2000), “VQ-based digital image watermarking method”, *Electron. Lett*, Vol. 36 (14), pp. 1201 – 1202.
- [56]. Xiangyang Luo, Bin Liu, and Fenlin Liu (2005), “Improved RS Method for Detection of LSB Steganography”, *ICCSA 2005*, LNCS 3481, pp. 508–516.
- [57]. Xiangyang Luo, Fenlin Liu (2007), “A LSB Steganography approach against pixel sample pairs Steganalysis”, *ICIC International @ 2007*, ISSN 1349-4198, pp. 575—588.
- [58]. B. Macq (2000), “Lossless Multi-Resolution Transform for Image Authenticating Watermarking”, *In Proc. of EUSIPCO*, Tampere, Finland.
- [59]. H. Malik (2008), “Steganalysis of QIM Steganography Using Irregularity Measure”, *MM&Sec'08*, Oxford, United Kingdom.
- [60]. L. Marvel, C. G. Boncelet Jr., and C. T. Retter (1999), “Spread spectrum image steganography”, *IEEE Trans. on Image Processing*, vol. 8 (8): pp. 1075-1083.

- [61]. Alfred J. Menezes, Scott A Vanstone (1996), *Handbook of Applied Cryptography*, CRC Press.
- [62]. Ni, Z., Shi, Y., Ansari, N., Su, W. (2003), “Reversible data hiding”, *Proc. ISCAS 2003*, pp. 912–915.
- [63]. Olson, D. L.; Delen, D. (2008), “Advanced Data Mining Techniques”, *Springer 1 edition*, ISBN 3540769161, page 138.
- [64]. S. Panchapakesan, N. Balakrishnan (1997), “Advances in Statistical Decision Theory and Applications, *Hamilton Printing, Rensselaer, NY*, ISBN 0 – 8176 – 3965 – 9, 3 – 7643 – 3965 – 9.
- [65]. F. A. P. Petitcolas, R. J. Anderson, and M.G. Kuhn (1999), “Information hiding – A survey”, *Proc. IEEE*, vol. 87 (7), pp. 1062 – 1078.
- [66]. Tomáš Pevný (2008), *Kernel Methods in Steganalysis*, Ph. D Thesis, Binghamton University, State University of New York.
- [67]. C. I. Podilchuk and E. J. Delp (2001), “Digital watermarking: Algorithms and applications”, *IEEE Signal Process. Mag.*, vol. 18 (4), pp. 33-34.
- [68]. V. Poor (1994), *An introduction to signal detection and estimation*, Springer - Verlag, New York.
- [69]. Niesl Provos, Peter Honeyman (2003), *Hide and seek: An introduction to steganography*, Published by The IEEE computer society.
- [70]. N. Provos (2001), “Defending Against Statistical Steganalysis”, *10th USENIX Security Symposium*, Washington.
- [71]. N. Provos and Peter Honeyman (2001), “Detecting Steganographic Content on the Internet”, *CITI Technical Report 01-11*, submitted for publication.
- [72]. M. Rabbani and R. Joshi (2002), “An Overview of the JPEG2000 Still Image Compression Standard”, *Signal Processing: Image Communication* 17, pp. 3–48.
- [73]. P. M. S. Raja, E. Baburaj (2011), “Survey of Steganographic Techniques in Network Security”, *International Journal of Research and Reviews in Computer Science (IJRRCS)*, Vol. 2 (1), pp. 98 – 103.

- [74]. Joseph Raphael A., Sundaram V. (2010), “Secured Communication through Hybrid Crypto-Steganography”, *International Journal of Computer Science and Information Security (IJCSIS)*, Vol. 8 (4), pp. 45-48.
- [75]. R. V. Schyndel, A. Tirkel, and C. Osborne (1994), “A digital watermark”, *In Proceedings of ICIP*, vol. 2, Austin, TX, pp. 86–90.
- [76]. Aubrey de Seslincourt (1996), *Herodotus - The Histories*, Penguin Books, London.
- [77]. T. Sharp (2001), “An implementation of key-based digital signal steganography”, *in Proc. 4<sup>th</sup> Int. Workshop Information Hiding*, Vol. 2137, Springer LNCS, pp. 13-26.
- [78]. C. A. Stanley (2005), *Pair of Values and the chi-Squared Attack*, Department of Mathematics, Iowa State University.
- [79]. J. P. Stern, G. Hachez, F. Koeune, and J. J. Quisquater (1999), “Robust Object watermarking Application to code”, *In proceedings of Info Hiding '99*, volume 1768, Lecture Notes in Computer Science, pp. 368-378.
- [80]. K. Sullivan, O. Dabeer, U. Madow, B. S. Manjunath and S. Chandrasekaran (Sep. 2003), “LLRT Based Detection of LSB Hiding”, *In Proc. IEEE International Conference on Image Processing (ICIP)*, Barcelona, Spain, pp. 497–500.
- [81]. K. Sullivan, Z. Bi, U. Madhow, S. Chandrasekaran and B.S. Manjunath (2004), “Steganalysis of quantization index modulation data hiding”, *In Proc. IEEE International Conference on Image Processing (ICIP)*, Singapore, pp. 1165–1168.
- [82]. K. Sullivan, U. Madhow, B. S. Manjunath, and S. Chandrasekaran (2005), “Steganalysis for Markov Cover Data with Applications to Images”, *Submitted to IEEE Transactions on Information Forensics and Security*.
- [83]. K. Sullivan, U. Madhow, S. Chandrasekaran and B. S. Manjunath (2005), “Steganalysis of Spread Spectrum Data Hiding Exploiting Cover Memory”, *In Proc. IS&T/SPIE's 17th Annual Symposium on Electronic Imaging Science and Technology*, San Jose, CA.

- [84]. K. M. Sullivan (2005), *Image steganalysis: Hunting and Escaping*, Ph. D Thesis in Electrical and computer Engineering, University of California.
- [85]. Ho Thi Huong Thom, Canh Ho Van, Tien Trinh Nhat (2009), “*Statistical Methods to Steganalysis of Color or Grayscale Images*”, *Proc. of IEEE-RIVF 2009 on Doctoral Symposium*, Da Nang University of Technology, pp. 1-5.
- [86]. Ho Thi Huong Thom, Ho Van Canh, Trinh Nhat Tien (2009), “Novel Algorithms to Steganalysis of Uncompressed and Compressed Images”, *Proceedings of KSE 2009 on Knowledge and Systems Engineering, College of Technology*, IEEE Computer Society, Vietnam National University, Ha Noi, pp. 87-92.
- [87]. Ho Thi Huong Thom, Ho Van Canh, Trinh Nhat Tien (2009), “Steganalysis to Reversible Data Hiding”, *Proceedings of FGIT 2009 on Database Theory and Application*, Springer-Verlag, Jeju, Korea, pp. 1- 6.
- [88]. Ho Thi Huong Thom, Canh Ho Van, Tien Trinh Nhat (2010), “Steganalysis of Reversible Vertical Horizontal Data Hiding Technique”, *International Journal of Computer Science and Information Security (IJCSIS)*, Vol. 8 (6), pp. 7-12.
- [89]. Huynh-Thu, Q.; Ghanbari, M. (2008), “Scope of validity of PSNR in image/video quality assessment”, *Electronics Letters 44*, pp. 800–801.
- [90]. J. Tian (2002), “Reversible Watermarking by Difference Expansion”, *In Proc. of Workshop on Multimedia and Security*, pp. 19-22.
- [91]. J. Tian (2002), “Wavelet Based Reversible Watermarking for Authentication”, *In Proc. Security and Watermarking of Multimedia Contents IV*, Electronic Imaging 2002, Vol. 4675, pp. 679-690.
- [92]. Y. Wang, P. Moulin (2003), “Steganalysis of Block-DCT Image Steganography”, *Proc. IEEE Workshop on Statistical Signal Processing 2003*.
- [93]. Shaowei Weng, Yao Zhao (2008), “A novel reversible data hiding scheme”, *International Journal of Innovative Computing, Information and Control*, Vol. 4 (3), pp. 351 – 358.

- [94]. A. Westfeld (2001), “High Capacity Despite Better Steganalysis (F5–A Steganographic Algorithm)”, *In: Moskowitz, I.S. (eds.): Information Hiding. 4th International Workshop*. Lecture Notes in Computer Science, Vol.2137. Springer-Verlag, Berlin Heidelberg New York, pp. 289– 302.
- [95]. A. Westfeld and A. Pfitzmann (1999), “Attacks on steganographic systems”, *In Lecture notes in computer science: 3rd International Workshop on Information Hiding*.
- [96]. A. Westfeld (2002), “Detecting Low Embedding rates”, *Preproceedings 5th Information Hiding Workshop*, Noordwijkerhout, Netherlands, pp. 7–9.
- [97]. H. C. Wu, N. I. Wu, C. S. Tsai, M. S. Hwang (2005), “Image Steganographic scheme based on pixel - value differencing and LSB replacement methods”, *IEE Proc.-Vis. Image Signal Process.*, Vol. 152, Issue 5, pp. 611 – 615.
- [98]. Guorong Xuan, Yun Q. Shi, Peiqi Chai, Xuefeng Tong, Jianzhong Teng, Jue Li (2008), “Reversible Binary Image Data Hiding By Run-Length Histogram Modification”, *The 19th International Conference on Pattern Recognition (ICPR 2008)*, Tampa, Florida, USA, pp 1 - 4.
- [99]. G. Xuan, Q. Yao, C. Yang, J. Gao, P. Chai, Y. Q. Shi, Z. Ni (2006), “Lossless Data Hidding Using Histogram Shifting Method Based on Integer Wavelets”, *Proc. 5th Digital watermarking workshop, IWDW 2006*, Korea, vol. 4283, pp. 323-332.
- [100].L. Yu, Y. Zhao, R. Ni, T.Li (2010), “Improved adaptive LSB steganography based on chaos and genetic algorithm”, *EURASIP Journal on Advances in Signal Processing - Special issue on advanced image processing for defense and security applications*, Vol. 2010.
- [101]. Xinpeng Zhang and Shuozhong Wang (2005), “Steganography Using Multiple-Base Notational System and Human Vision Sensitivity”, *IEEE Signal Processing Letters*, Vol. 12 (1), pp. 67 – 70.
- [102]. T. Zhang and X. Ping (2003), “Reliable detection of LSB steganography based on the difference image histogram”, *IEEE International Conferenceon Acoustics, Speech, and Signal Processing*, Volume 3, pp.545-548.

**Trang Web**

- [103]. CBIR image database, University of Washington, available at: <http://www.cs.washington.edu/research/imagedatabase/groundtruth/>
- [104]. Derek Upham: Jsteg (1997), “<http://www.tiac.net/users/Korejwa/Jsteg.htm>”.
- [105]. Romana Machado (1996), EzStego, “<http://www.stego.com>”.
- [106]. StegoArchive.com: “<http://www.stegoarchive.com>”.
- [107]. USC-SIPI Image Database, Signal and Image Processing Institute, University of Southern California, <http://sipi.usc.edu/services/database/Database.html>

### **Tiếng Nga**

- [108]. С. Р. ПАО (1968), *Линейные статистические методы и их применение*, Москва.
- [109]. Л.Н. Большев, Н.В.Смирнов (1983), *Таблицы Математической Статистики*, Наука Москва.
- [110]. Римский (1960), Л. З., *Элементы теории вероятностей*, физматгиз.

# PHỤ LỤC – CHƯƠNG TRÌNH ĐỀ MÔ GIẤU TIN TRONG ẢNH VÀ PHÁT HIỆN ẢNH CÓ GIẤU TIN

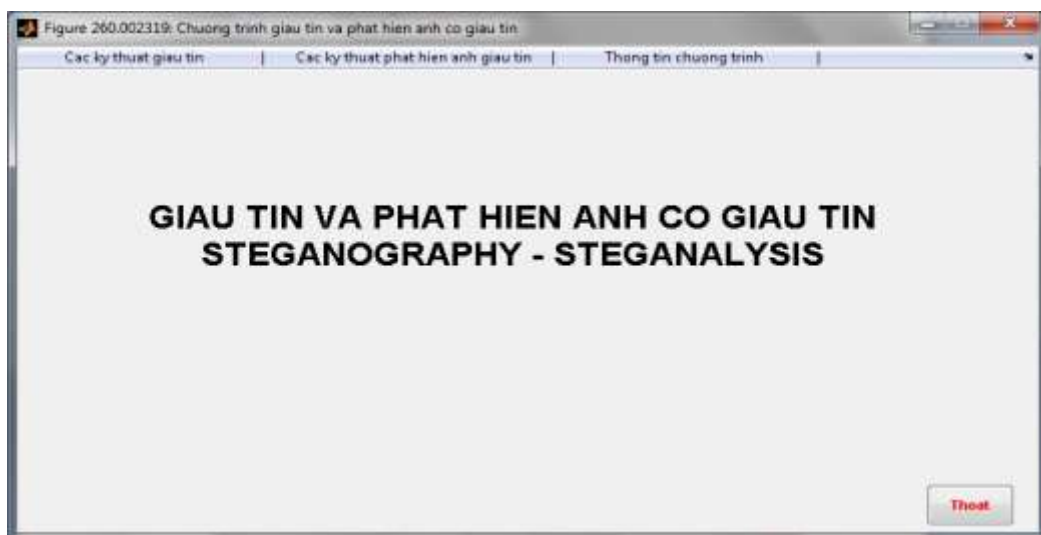
Phụ lục này đề mô chương trình giấu tin và phát hiện ảnh có gồm hai mô đun chính: Giấu thông tin trong ảnh và phát hiện ảnh có giấu tin. Đây là các mô đun phục vụ cho quá trình thử nghiệm các kỹ thuật giấu và phát hiện với các chức năng tương đối đầy đủ, giao diện thân thiện để sử dụng.

## 1. Môi trường cài đặt

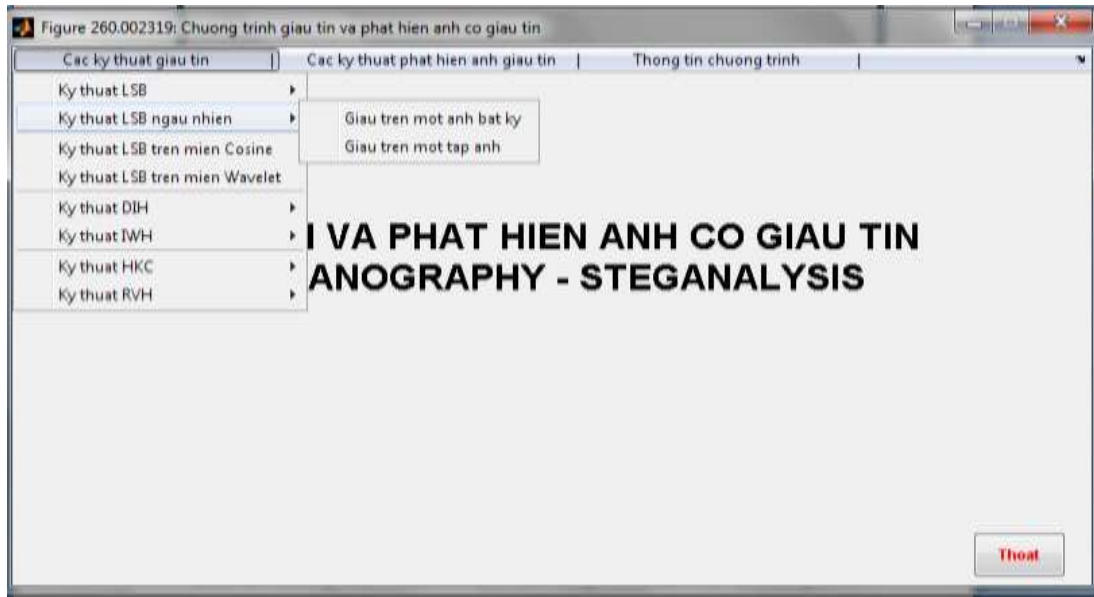
Các thử nghiệm dùng để đánh giá thuật toán và kỹ thuật giấu và phát hiện được thực hiện trên môi trường chung là Matlab phiên bản 2008b. Môi trường này hỗ trợ nhiều tính năng liên quan đến đọc và lưu dữ liệu ảnh vì vậy giúp giảm thiểu việc xử lý vào ra đối với các tệp ảnh.

## 2. Giao diện chương trình

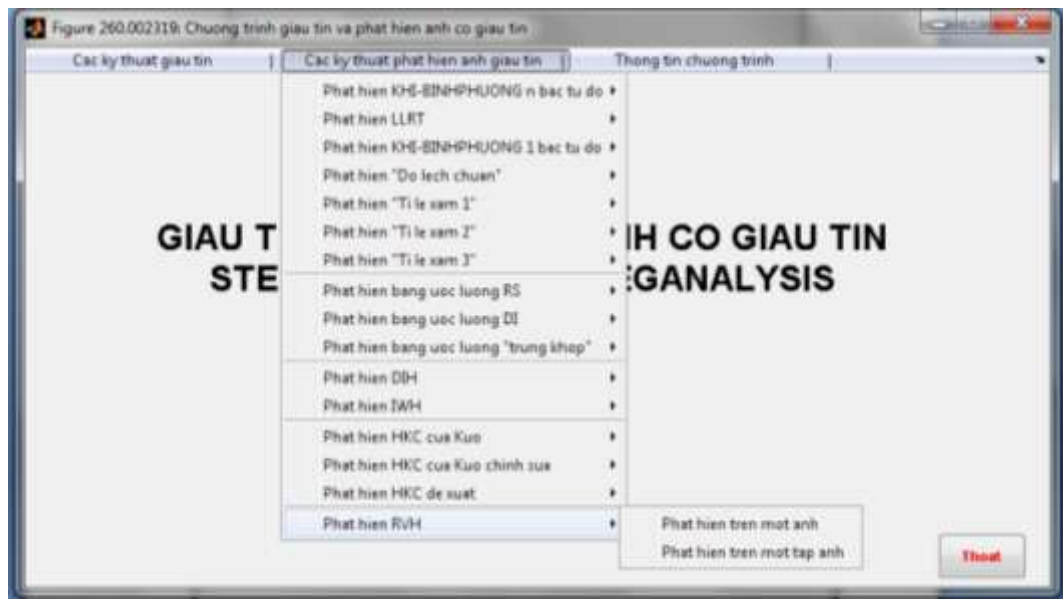
Sau đây là một số cửa sổ giao diện chính của chương trình. Cửa sổ chính của chương trình (hình 1) có 2 module chính là module các kỹ thuật giấu tin và các kỹ thuật phát hiện ảnh có giấu tin như hình 2 và hình 3. Các hình tiếp theo là ví dụ minh họa chi tiết thực hiện của một số chức năng giấu tin, tách tin, kiểm tra một ảnh bất kỳ hay một tập ảnh bất kỳ có giấu tin hay không.



**Hình B.1.** Giao diện chương trình chính

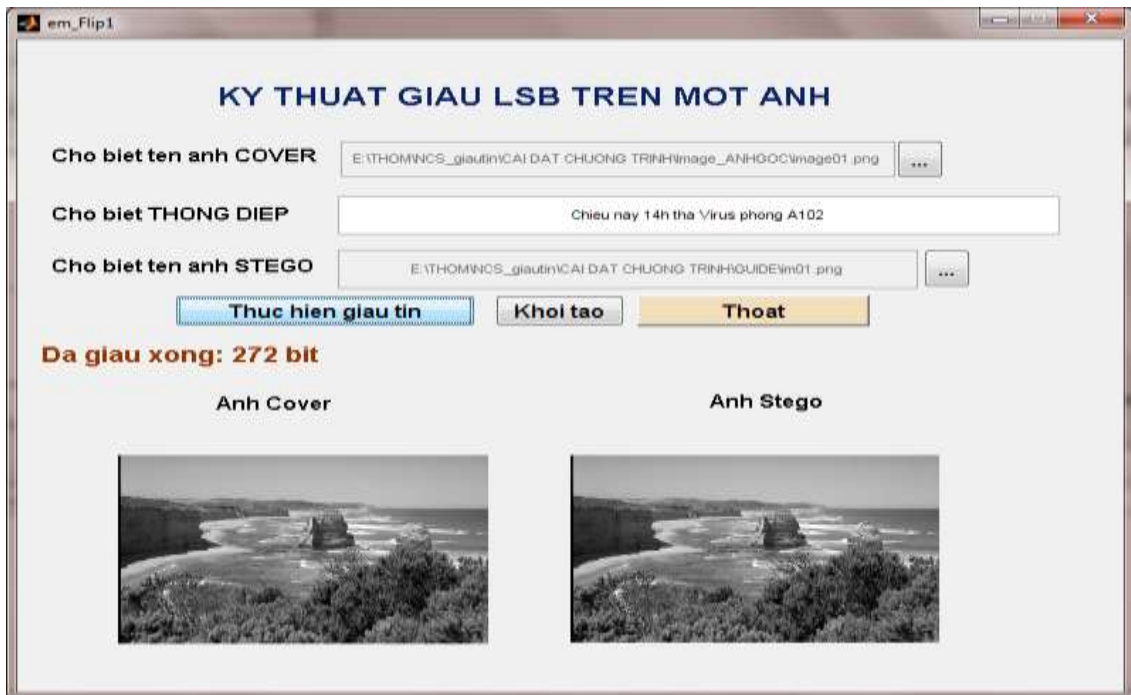


Hình B.2. Chương trình chính với các chức năng của menu *Các kỹ thuật giấu tin*



Hình B.3. Các chức năng của menu *Các kỹ thuật phát hiện ảnh giấu tin*

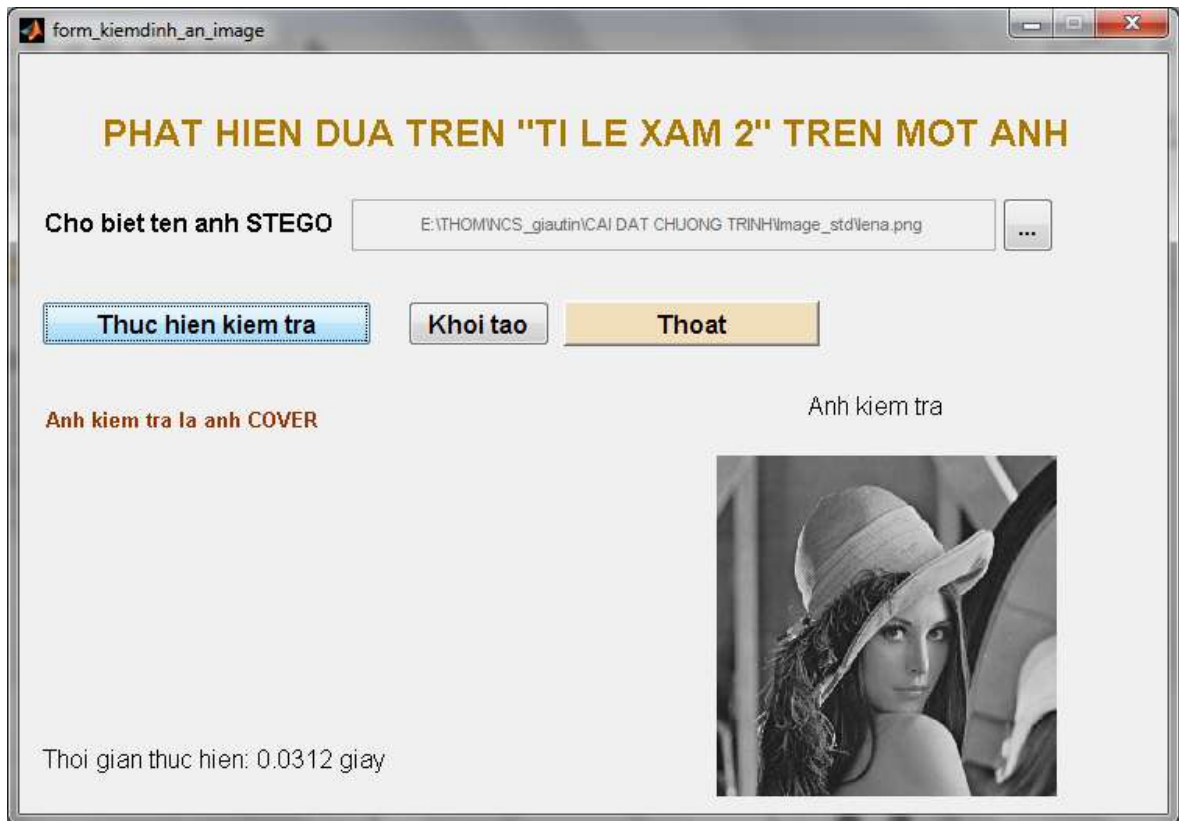




**Hình B.4.** Cửa sổ giao diện kỹ thuật giấu LSB trên một ảnh



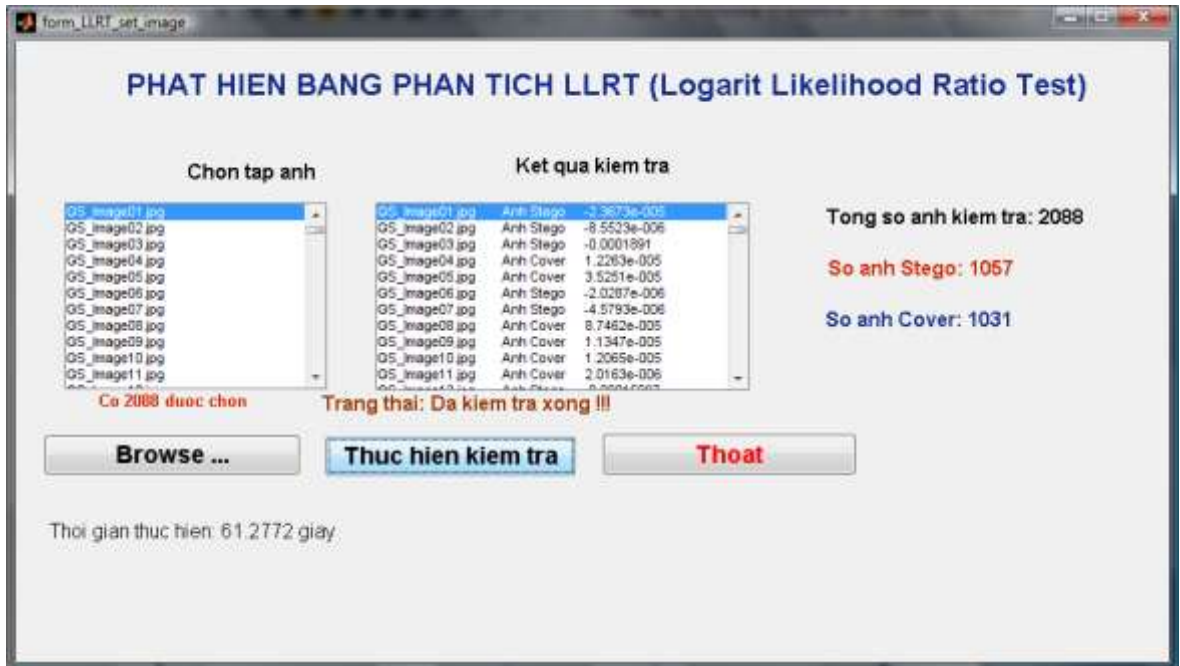
**Hình B.5.** Giao diện giấu thông tin giấu bằng LSB trên một tập ảnh với thông tin giấu được sinh ngẫu nhiên



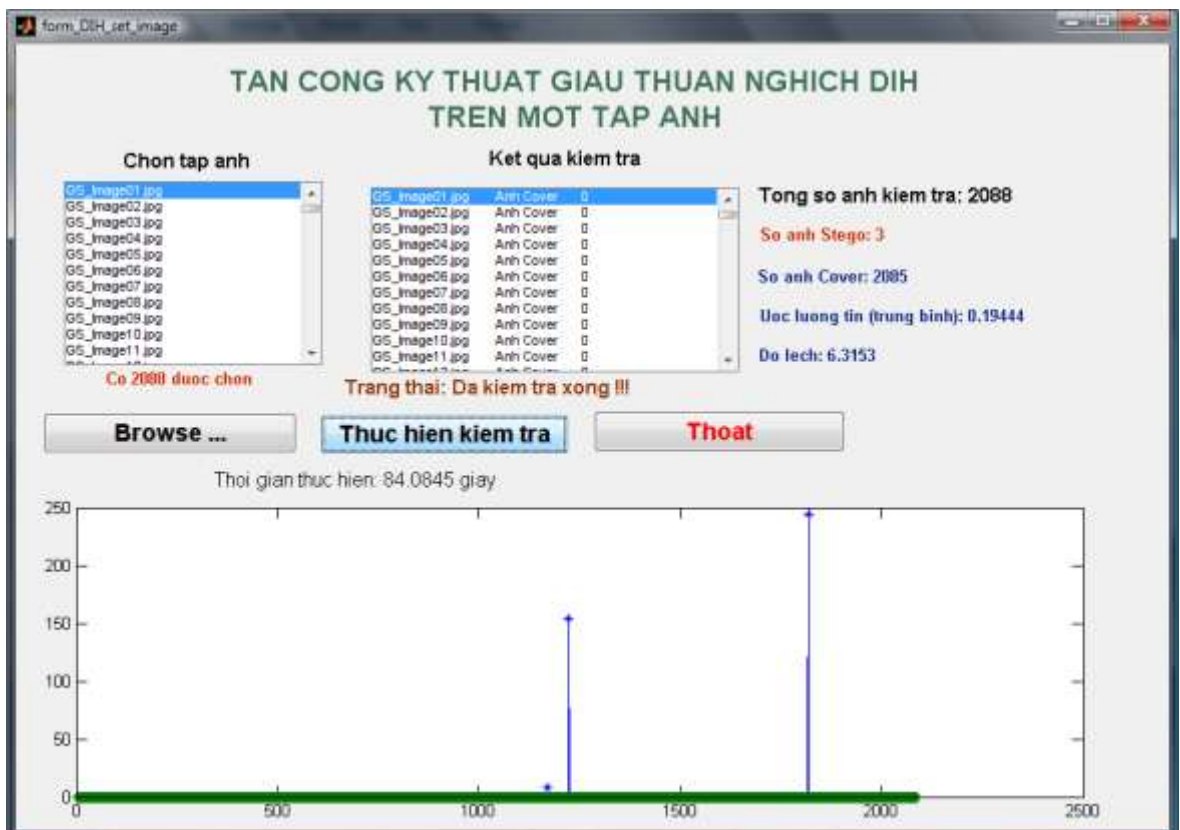
Hình B.6. Giao diện kiểm tra ảnh Lena.png bằng “tỉ lệ xám 2”



Hình B.7. Giao diện kiểm tra tập ảnh gốc  $C_0$  (2088 ảnh gốc) bằng “tỉ lệ xám 2”



**Hình B.8.** Giao diện kiểm tra tập ảnh gốc  $\mathcal{C}_0$  (2088 ảnh gốc) bằng kỹ thuật LLRT



**Hình B.9.** Giao diện kiểm tra và ước lượng thông tin giấu bằng kỹ thuật phát hiện ảnh có giấu tin sử dụng kỹ thuật DIH cho tập ảnh  $\mathcal{C}_0$  (gồm 2088 ảnh gốc)

### 3. Danh mục các chức năng của chương trình

#### a. Mô đun giấu tin

Mô đun này bao gồm các chức năng giấu thông tin cho các kỹ thuật giấu sau:

- *Kỹ thuật giấu tin LSB* (các điểm ảnh được chọn tuần tự): Giấu trên một ảnh với thông tin là một đoạn văn bản; Tách thông tin trên một ảnh. Có thể thực hiện giấu cùng lúc trên một tập ảnh

- *Kỹ thuật giấu tin LSB ngẫu nhiên*: Tương tự như kỹ thuật giấu LSB ở trên tuy nhiên thay vì các điểm ảnh giấu tin sẽ thực hiện một cách chọn ngẫu nhiên trong toàn ảnh, phục vụ cho trường hợp phát hiện tổng quát. Gồm chức năng giấu trên một ảnh và giấu trên một tập ảnh.

- *Kỹ thuật giấu tin LSB trên miền tần số cosine*: Tương tự như kỹ thuật giấu LSB ở trên tuy nhiên thay vì các điểm ảnh giấu tin sẽ thực hiện giấu trên các hệ số cosine. Gồm chức năng giấu trên một ảnh và giấu trên một tập ảnh.

- *Kỹ thuật giấu tin LSB trên miền tần số wavelet*: Chức năng giấu thông tin trên LSB của các hệ số wavelet. Gồm chức năng giấu trên một ảnh và giấu trên một tập ảnh.

- *Kỹ thuật giấu tin DIH*: Giấu trên một ảnh (cả quy trình tách tin trên một ảnh), giấu cùng thông tin trên một tập ảnh với độ dài nhập vào (thông tin được sinh ngẫu nhiên từ độ dài cho biết)

- *Kỹ thuật giấu tin IWH*: Giấu trên một ảnh (cả quy trình tách tin trên một ảnh), giấu thông tin trên một tập ảnh

- *Kỹ thuật giấu tin HKC*: Giấu thông tin trên một ảnh và trên một tập ảnh

- *Kỹ thuật giấu tin RVH*: Giấu thông tin trên một ảnh và trên một tập ảnh

#### b. Mô đun phát hiện ảnh có giấu tin

Mô đun này bao gồm các chức năng phát hiện ảnh có giấu tin: Mỗi chức năng phát hiện cho một phương pháp đều có thể thực hiện trên từng ảnh và trên một tập ảnh để thuận tiện kiểm tra đánh giá, chi tiết gồm có các chức năng sau:

- *Kỹ thuật phát hiện khi-bình phương với  $n$  bậc tự do*: Cho cả miền không gian và miền tần số (cosine, wavelet).

- *Kỹ thuật phát hiện LLRT*.

- *Kỹ thuật phát hiện khi-bình phương một bậc tự do*.

- Kỹ thuật phát hiện bằng độ lệch chuẩn.
- Kỹ thuật phát hiện dựa trên thống kê “tỉ lệ xám 1”.
- Kỹ thuật phát hiện dựa trên thống kê “tỉ lệ xám 2”.
- Kỹ thuật phát hiện dựa trên thống kê “tỉ lệ xám 3” trên miền tần số (cosine, wavelet).
- Kỹ thuật phát hiện và ước lượng thông tin RS.
- Kỹ thuật phát hiện và ước lượng thông tin DI.
- Kỹ thuật phát hiện ước lượng trùng khớp.
- Kỹ thuật phát hiện HKC của Kuo và Lin.
- Kỹ thuật phát hiện HKC của Kuo và Lin cải tiến.
- Kỹ thuật phát hiện HKC đề xuất khác.
- Kỹ thuật phát hiện DIH.
- Kỹ thuật phát hiện IWH.
- Kỹ thuật phát hiện RVH.