ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN
KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG

ẨN THÔNG TIN TRÊN DỮ LIỆU SỐ VÀ ỨNG DỤNG

CÁC KỸ THUẬT ẨN GIẤU THÔNG TIN TRONG ỨNG DỤNG VÀ DỮ LIỆU

TÔ TRỌNG NGHĨA
NGUYỄN HỒNG SƠN
PHẠM TRẦN TIẾN ĐẠT
TẠ VIỆT HOÀNG

GIẢNG VIÊN HƯỚNG DẪN
TS. NGUYỄN NGỌC TỰ

TP. HỒ CHÍ MINH, NĂM 2023

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN
KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG

NGUYỄN HỒNG SƠN - 220202022
TÔ TRỌNG NGHĨA - 220202019
PHẠM TRẦN TIẾN ĐẠT - 220202017
TẠ VIỆT HOÀNG - 220202018

ẨN THÔNG TIN TRÊN DỮ LIỆU SỐ VÀ ỨNG DỤNG

CÁC KỸ THUẬT ẨN GIẤU THÔNG TIN TRONG ỨNG DỤNG VÀ DỮ LIỆU

GIẢNG VIÊN HƯỚNG DẪN
TS. NGUYỄN NGỌC TỰ

TP. HỒ CHÍ MINH, NĂM 2023

Mục lục

Danh sách hình vẽ

Danh sách bảng

Tóm tắt đề tài

Sự phát triển của công nghệ mạng và truyền thông trong kỷ nguyên hiện đại đã làm tăng tốc độ truyền tải lên gấp hàng ngàn lần. Dữ liệu truyền tài trên mạng máy tính luân chuyển liên tục, đòi hỏi sự an toàn cho chúng.

An toàn thông tin trong lĩnh vực này chia thành mã hóa thông tin và ẩn giấu thông tin. Mã hóa thông tin chuyển đổi những dữ liệu bí mật thành loại dữ liệu khác mà kẻ tấn công không thể đọc được nó. Tuy vậy, dữ liệu mã hóa trở thành ốc đảo giữa sa mạc, gây sự chú ý rất lớn từ kẻ tấn công.

Do đó, một kỹ thuật khác nhằm bảo vệ dữ liệu là che giấu chính sự tồn tại của bí mật đó trước kẻ tấn công. Các dữ liệu được nhúng và gần như tàng hình trước kẻ xấu, và như vậy ít gây chú ý hơn. Trong lĩnh vực này, chia thành hai nội dung với những mục đích khác nhau. Trong khi kỹ thuật giấu tin ẩn vào dữ liệu được thực hiện nhằm mục đích bảo vệ sự bí mật của "dữ liệu được giấu" thì kỹ thuật watermark lại có mục đích bảo vệ chính dữ liệu đó. Với khả năng rút trích dữ liệu được giấu từ phiên bản số, ta dễ dàng chứng minh được tác quyền với nó [2].

Do có những ứng dụng đặc thù như vậy, ẩn thông tin vẫn là một hướng nghiên cứu lớn. Mặc dù không thể so sánh được với những hướng đi đang nổi lên trong giai đoạn gần đây như máy học, dữ liệu lớn... nó vẫn duy trì và đi từng bước mạnh mẽ. Phần còn lại của đề tài giới thiệu một số công trình nghiên cứu trong lĩnh vực ẩn dữ liệu bao gồm:

- **Chương 1** giới thiệu phương pháp LSB sử dụng hàm 1D chaotic map đã được cải thiện do nhóm tác giả Chanil Pak [4]. Trong công trình này, nhóm tác giả đề xuất hàm 1D chaotic map mới đã được cải thiện, từ đó tạo

ra các phương trình nhúng và giải nén hiệu quả hơn nhiều so với phương pháp cũ.

- **Chương 2** do nhóm tác giả Suah Kim[3] đề xuất một phương pháp ẩn dữ liệu có thể đảo ngược mới mà có thể nhúng thông tin một cách hiệu quả trong DC. Phương pháp đề xuất sử dụng một phương pháp dự đoán DC mới để giảm entropi của prediction error histogram.

Chương 1

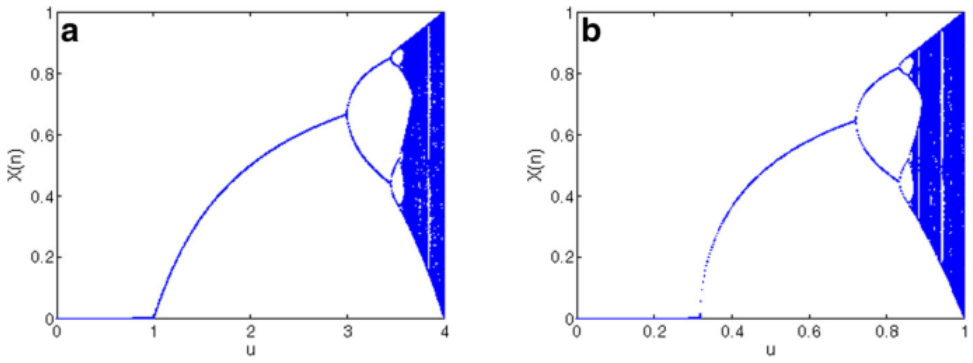
LSB steganography using improved 1D chaotic map

Least Significant Bit (LSB) Steganography là một kỹ thuật trong lĩnh vực ẩn giấu thông tin, được sử dụng để nhúng thông tin bí mật vào trong một tập tin đa phương tiện, chẳng hạn như hình ảnh, âm thanh hoặc video. Kỹ thuật này tận dụng tính chất của các bit ít quan trọng nhất (Least Significant Bits) trong các dữ liệu số như điểm ảnh, mẫu âm thanh hoặc khung hình video. LSB Steganography cho phép nhúng thông tin ẩn vào những bit ít quan trọng này mà không gây ra sự thay đổi đáng kể cho dữ liệu gốc.

Nguyên tắc hoạt động của LSB Steganography rất đơn giản: trong một tập tin đa phương tiện, các dữ liệu như điểm ảnh thường được biểu diễn bằng các chuỗi bit. Các bit ít quan trọng nhất thường có giá trị thấp hơn và có xu hướng thay đổi ít ảnh hưởng đến hình ảnh hoặc âm thanh tổng thể. Điều này tạo ra một cơ hội tốt để thay thế những bit này bằng các bit của thông tin ẩn, giữ nguyên tính nguyên vẹn của dữ liệu gốc mà vẫn chèn thông tin bí mật vào.

1.1 Chaotic map

Chaotic map được chia thành map một chiều (1D) và đa chiều (multi-dimensional). Nó thường được sử dụng trong mã hóa vì nó có tính ngẫu nhiên của chuỗi hỗn loạn được tạo. Mặc dù phiên bản 1D có một số nhược điểm nhưng chúng được



Hình 1.1: Logistic map (a) và sine map (b)

sử dụng rộng rãi do cấu trúc đơn giản và chi phí tính toán thấp, các nghiên cứu đang được thực hiện để cải thiện hiệu suất của nó.

1.1.1 Logistic và sine map hiện tại

Logistic map hiện tại có thể biểu diễn đơn giản như sau:

$$x_{n+1} = u \times x_n \times (1 - x_n) \tag{1.1}$$

trong đó $u \in [0,4\}$ là tham số điều khiển của hàm chaotic và $x_0 \in [0,1\}$ là giá trị ban đầu của nó.

Sine map hiện tại được thể hiện như sau:

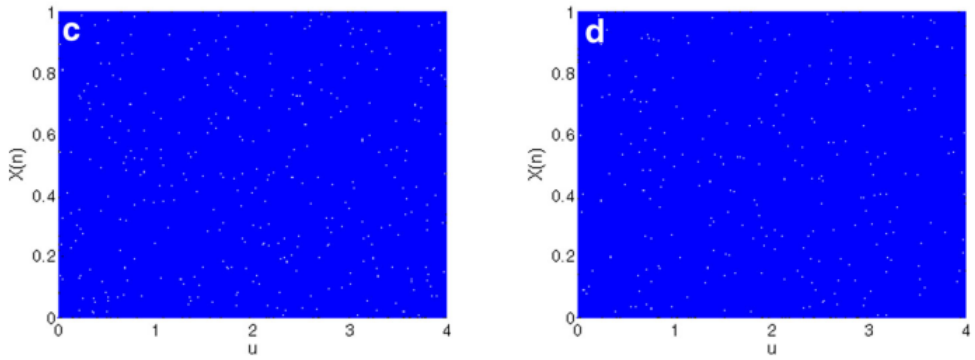
$$x_{n+1} = r \times \sin(\pi \times x_n) \tag{1.2}$$

trong đó $r \in (0,1]$ là tham số điều khiển của sine map. Sine map và logistic map thể hiện trong **Hình 1.1**

1.1.2 Improved 1D chaotic system model

Hàm 1D chaotic được cải tiến được thể hiện như sau:

$$\begin{aligned} f_{ic}(u, x_{n+1}, k) &= mod(f_c(u, x_n) \times g(k), 1). \\ & where g(k) = 2^k, 9 \leq k \leq 16. \end{aligned} \tag{1.3}$$



Hình 1.2: Distribubtions của hai hàm logisctic map (c) và sine map

Tham số hệ thống u vẫn nằm trong đoạn $(0,4]$ và có thể mở rộng thêm. $f_c(u,x_n)$ là hàm 1D chaotic map hiện tại, $f_{ic}(u,x_{n+1},k)$ là hàm đã được cải tiến của mô hình đề xuất. $k = 12$ là giá trị tốt nhất (sau khi đã thực nghiệm).

1.1.3 Improved 1D chaotic map and performance evaluation

Dựa trên những cải tiến của hàm chaotic tại 1.3, hàm logistic map được thể hiện như sau:

$$x_{n+1} = mod(u \times x_n \times (1 - x_n) \times 2^{12}, 1) \tag{1.4}$$

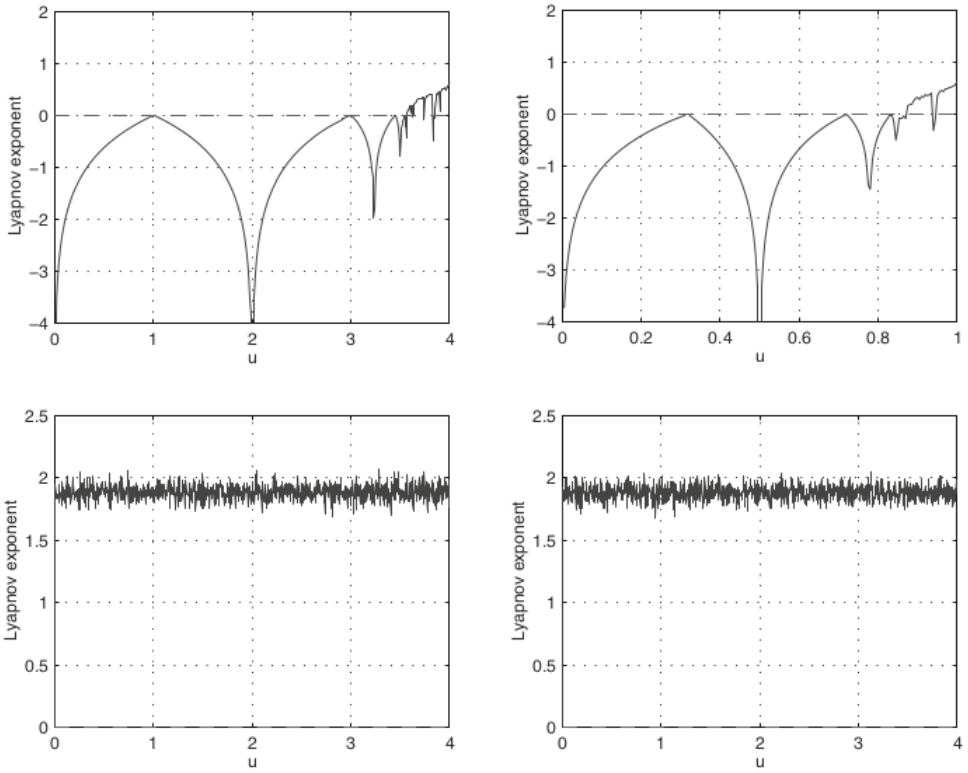
và hàm sine map được cải tiến như sau:

$$x_{n+1} = mod(u \times \sin(\pi \times x_n) \times 2^{12}, 1) \tag{1.5}$$

Hình 1.2 mô tả phân bố của các hàm logistic và sine sau khi cải tiến hàm chaotic.

Số mũ Lyapunov là một chỉ số để đánh giá hiệu suất của chaotic map và có các đặc tính hỗn loạn tốt khi giá trị lớn hơn 0. Số mũ Lyapunov của chaotic map hiện tại và của phiên bản cải thiện được thể hiện trong **Hình 1.3**.

Ngoài ra, entropy là chỉ số đánh giá hiệu suất của chaotic map, là một chỉ số để đánh giá sự không ổn định của các giá trị ngẫu nhiên, có nghĩa là nó có tối đa giá trị khi tất cả các tín hiệu được phân phối ngẫu nhiên và giá trị càng gần với 8 thì đặc tính phân phối càng tốt. Hàm entropy, được thể hiện trong công thức



Hình 1.3: Biểu đồ số mũ Lyapunov logistic map (a), sine map (b) và phiên bản cải tiến của nó

sau

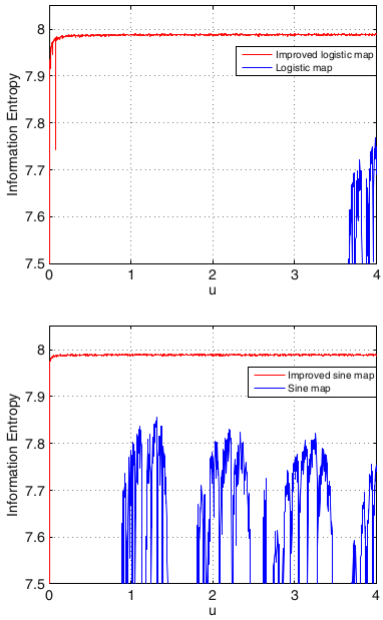
$$I(R) = \sum_{i=0}^{F-1} P(R=i) \times \log_2 P(R=i) \tag{1.6}$$

trong đó P là hàm mật độ xác suất rời rạc. **Hình 1.4** cho thấy sự tương phản giữa chỉ số entropy chaotic map hiện có và phiên bản được cải tiến. Nó cho thấy rằng chaotic map được cải thiện có các đặc điểm phân phối hoàn toàn vượt trội. Các kết quả thử nghiệm này cho thấy mô hình hệ 1D chaotic system được đề xuất là rất chính xác.

1.2 Proposed LSB steganography algorithm

1.2.1 Embedding process

Quá trình nhúng là một quá trình ẩn dữ liệu bí mật trong ảnh bìa và các tệp hình ảnh và văn bản có thể được sử dụng làm dữ liệu bí mật. Thuật toán như



Hình 1.4: Chỉ số entropy của hàm hiện tại (a) và bản cải ttiến

sau.

- **Bước 1**: Đọc ảnh bìa và dữ liệu bí mật. Đọc ảnh bìa và lấy giá trị pixel trung bình của ảnh bìa theo phương trình sau

$$PM_c = \sum_{k=1}^{c} \sum_{i=1}^{M} \sum_{j=1}^{n} cp_{ij} \,/\, (c \times M \times N) \tag{1.7}$$

  với $c = 3$ là giá trị của bảng màu RGB, M và N là chiều cao và chiều rộng của ảnh bìa và cp_{ij} là giá trị pixel của ảnh bìa. Tiếp theo, dữ liệu bí mật được nhúng được đọc và chuyển đổi thành ma trận một chiều và giá trị trung bình của dữ liệu bí mật thu được theo phương trình sau.

$$PM_s = \sum_{i=1}^{sLen} sd_i \,/\, sLen \tag{1.8}$$

  với sd_i là giá trị phần tử ma trận một chiều của dữ liệu bí mật và sLen là độ dài dữ liệu bí mật.

- **Bước 2:** Xác định các tham số ban đầu của chaotic map và tạo khóa. Từ giá trị PM_c và PM_s được tính tại **Bước 1**, các tham số ban đầu của chaotic

map được tính toán như sau.

$$x'_0 = x_0 \times PM_c - floor(x_0 \times PM_c) \tag{1.9}$$

$$u' = 4 \times (u \times PM_s - floor(u \times PM_s)) \tag{1.10}$$

với $u' \in [0,4], x'_0 \in [0,1]$ Bằng cách đặt x'_0 và u' được tính toán lại làm tham số hệ thống ban đầu của 1D chaotic map bản cải tiến, chúng ta có thể rút ra chuỗi $XM = \{x_1, x_2, ...x-s\}$ có kích thước s được tính theo phương trình 1.11 và $bc_{lsb} = 4$ là số bit LSB của ảnh bìa.

$$s = (c \times M \times N \times bc_{lsb}) \tag{1.11}$$

- **Bước 3:**Tính toán ma trận vị trí nhúng. Chúng ta có ma trận vị trí $P = \{p_1, p_2, ...p_s\}$ bằng cách sắp xếp đầu ra của chaotic map XM theo quy trình tại **Hình 1.6** Từ ma trận vị trí P, chúng ta tính toán được ma trận nhúng $EP = \{ep_1, ep_2, ...ep_s\}$ với $ep_i = \{p_{cp}(i), p_{row}(i), p_{col}(i)\}$ được tính theo các phương trình 1.12, 1.13, 1.14

$$p_{cp}(i) = floor((p(i)-1) \,/\, (M \times N)) + 1 \tag{1.12}$$

$$p_{row}(i) = mod((p(i)-1), N) + 1 \tag{1.13}$$

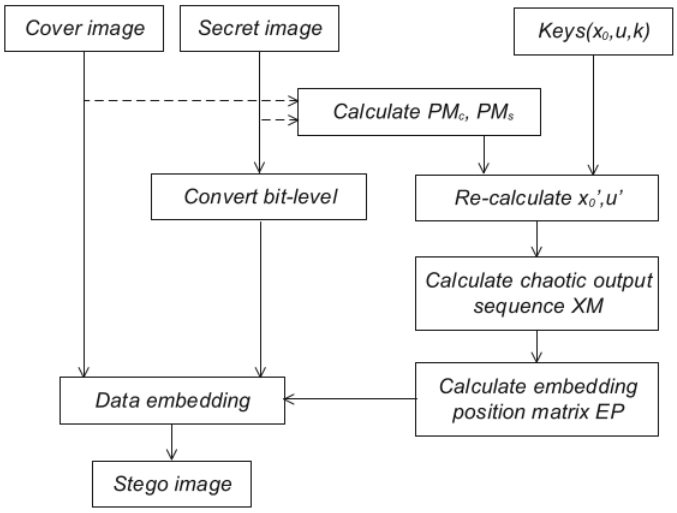
$$p_{col}(i) = mod((floor((p(i)-1) \,/\, M), N) + 1 \tag{1.14}$$

với $1 \leq p_{cp}(i) \leq c, 1 \leq p_{row}(i) \leq M, 1 \leq p_{col}(i) \leq N$. $p_{cp}(i)$là số bảng màu của vị trí nhúng dữ liệu bí mật, $p_{row}(i)$ là vị trí hàng được nhúng và $p_{col}(i)$ là vị trí cột. Phương trình 1.12 - 1.14 được tính toán lặp đi lặp lại theo s lần và ma trận vị trí nhúng thu được cung cấp tất cả thông tin về các vị trí nhúng dữ liệu bí mật.

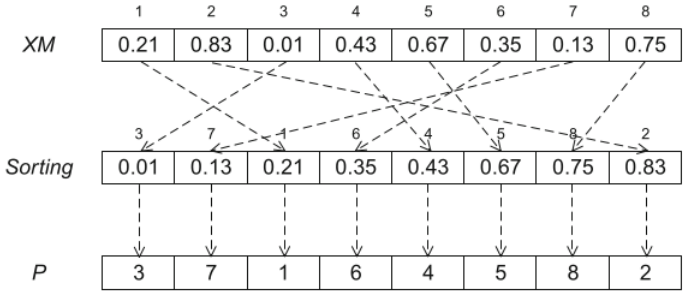
- **Bước 4**: Quy trình nhúng Đầu tiên tạo ma trận bit một chiều $sb = \{sb_1, sb_2, ...sb_{sLen}\}$ của dữ liệu bí mật. Theo ma trận EP được tính toán tại **Bước 3**, bốn bit của sb ma trận sẽ được nhúng trong các bit LSB của ảnh bìa dưới dạng một đơn vị và quá trình này có thể được biểu diễn như sau.

$$cp_{lsb}(p_{cp}(i), p_{row}(i), p_{col}(i)) = sb(i \times 4 - 3 : i \times 4) \tag{1.15}$$

với $1 \leq i \leq (2 \times sLen)$ và cp_{lsb} là bit LSB của ảnh bìa.



Hình 1.5: Lưu đồ tổng thể thuật toán đề xuất



Hình 1.6: Sơ đồ sinh ma trận vị trí

Bước 4 thực hiện $(2 \times sLen)$ lần tới chừng nào hình ảnh stego hoàn thành. Trong trường hợp dữ liệu bí mật được nhúng là một hình ảnh, cần phải chuyển đổi dữ liệu hình ảnh bí mật sang ma trận một chiều ở **Bước 1**

1.2.2 Extracting process

Ở giai đoạn này, trích xuất dữ liệu bí mật được chèn vào hình ảnh stego và nó có thể được coi là quá trình ngược lại với quy trình nhúng. $(x_0, u_0, k, PM_c, PM_s, sLen)$ là các khóa bí mật và quá trình trích xuất có thể được biểu diễn như sau.

$$sb(i \times 4 - 3 : i \times 4) = cp_{lsb}(p_{cp}(i), p_{row}(i), p_{col}(i)) \tag{1.16}$$

với $1 \leq i \leq (2 \times sLen)$. Ma trận bit thu được bằng cách lặp lại $(s \times sLen)$ lần được chuyển thành ma trận byte. Do đó, thông tin bí mật ban đầu thu được.

Trường hợp dữ liệu bí mật được nhúng là ảnh thì cần chuyển ma trận một chiều thu được thành ma trận hai chiều tương ứng với kích thước của ảnh mật.

Chương 2

Reversible Data Hiding in JPEG Images Using Quantized DC

2.1 Introduction

Các hệ số DC (hệ số dòng điện một chiều lượng tử hóa) không được sử dụng để nhúng do người ta cho rằng việc nhúng DC gây ra nhiều méo mó hơn so với việc nhúng trong các hệ số AC. Tuy nhiên, đối với phân tích dữ liệu trích xuất các yếu tố chi tiết như trích xuất đặc trưng thì sự méo mó trong các hệ số AC là không chấp nhận được.

Định dạng JPEG đã khẳng định vị thế ưu việt của mình qua từng năm. Ngay cả khi có nhiều tiêu chuẩn hình ảnh mới hỗ trợ hiệu suất và nén cao hơn, JPEG vẫn là tiêu chuẩn hình ảnh mặc định trên điện thoại và máy tính. Với sự hỗ trợ phi thường trên đa dạng thiết bị và phần mềm, việc ẩn dữ liệu có khả năng đảo ngược trong hình ảnh JPEG đã trở thành một chủ đề quan trọng.

Ẩn dữ liệu có khả năng đảo ngược là một phương pháp ẩn dữ liệu tương thích, duy trì định dạng file gốc và có khả năng khôi phục hình ảnh ban đầu từ hình ảnh đã nhúng hoặc watermarked. Tuy nó khác với *robust watermarking scheme* mạnh mẽ như lược đồ được đề xuất bởi Liu và cộng sự [1] tập trung vào việc khôi phục thông điệp đã nhúng dưới các kiểu tấn công xử lý hình ảnh.

Hình ảnh đã nhúng cần giống với hình ảnh gốc càng nhiều càng tốt, và giá trị PSNR được đo đạc đối với các kích thước payload khác nhau để so sánh hiệu suất của khả năng ẩn dữ liệu.

Hầu hết các nghiên cứu về ẩn dữ liệu có khả năng đảo ngược tập trung vào miền điểm ảnh (pixel domain). Chúng dựa trên kỹ thuật *lossless compression, difference expansion* hay *histogram shifting*. Gần đây nhiều công trình đã sử dụng kỹ thuật dịch chuyển biểu đồ hai chiều (two dimensional histogram shifting) để đạt được khả năng nhúng cao hơn và méo mó thấp hơn. Hơn nữa, đã xuất hiện một lĩnh vực nghiên cứu mới sử dụng ẩn dữ liệu có khả năng đảo ngược, tập trung vào việc biến nó như một kỹ thuật tăng cường hình ảnh.

Đặc biệt, một số nghiên cứu đã đề xuất sử dụng kỹ thuật này để tăng cường hình ảnh tự động và tiết kiệm không gian lưu trữ. Ẩn dữ liệu có khả năng đảo ngược cũng có thể được sử dụng trước khi mã hóa hình ảnh để ẩn dữ liệu bổ sung hoặc làm mờ kích thước của hình ảnh.

Tuy nhiên, ẩn dữ liệu có khả năng đảo ngược trong JPEG chưa được nghiên cứu một cách rộng rãi. Có ba phương pháp chính:

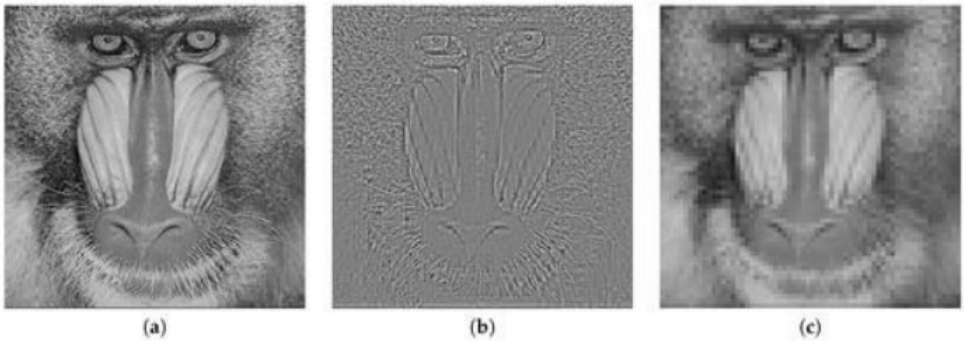
- **Phương pháp đầu tiên:** sửa đổi quantization table để tăng cường hệ số DCT được lượng hóa (quantized). Mặc dù phương pháp này có khả năng nhúng cao, nhưng nó tăng kích thước tệp lớn hơn rất nhiều so với khả năng nhúng thu được.

- **Phương pháp thứ hai:** sửa đổi bảng Huffman. Mặc dù phương pháp này duy trì kích thước file nhưng bù lại khả năng nhúng khá hạn chế.

- **Phương pháp thứ ba:** sửa đổi nhân tố DCT được lượng hóa để nhúng. Đây là phương pháp logic nhất vì nó sửa đổi trực tiếp các đặc điểm hình ảnh mà không sửa đổi các thông số như bảng Huffman và bảng lượng hóa.

Phương pháp đề xuất là một phương pháp thứ ba, sử dụng một mô hình dự đoán cho các hệ số DC được lượng hóa. Mô hình dự đoán đề xuất cung cấp độ chính xác cải thiện, giúp giảm entropi của quantized DC prediction error histogram để có khả năng nhúng lớn với méo mó thấp hơn. Hơn nữa, phương pháp đề xuất chỉ sửa đổi các giá trị hệ số DC được lượng hóa.

Mục tiêu chính của kỹ thuật này là đạt được PSNR cao mà không gây ra nhiều thay đổi trong kích thước tệp. Phân tích dữ liệu hình ảnh, phụ thuộc vào



Hình 2.1: Hình ảnh JPEG tái xây dựng con tinh tinh bằng cách sử dụng các tập hợp khác nhau của các hệ số DCT đã được lượng tử hóa.

việc trích xuất đặc điểm của các chi tiết mà các hệ số AC biểu thị. **Hình 2.1** mô tả tái xây dựng con tinh tinh bằng cách sử dụng các tập hợp khác nhau của các hệ số DCT đã được lượng tử hóa. Các hệ số DC đã được lượng tử hóa bảo tồn tổng cường độ chung, trong khi các hệ số AC bảo tồn các chi tiết của hình ảnh, làm cho chúng ít lý tưởng hơn khi nhúng dữ liệu. (a) tất cả các hệ số DCT đã được lượng tử hóa; (b) các hệ số AC đã được lượng tử hóa; (c) các hệ số DC đã được lượng tử hóa.. Nếu không có sự bảo tồn hệ số AC, phân tích dữ liệu có thể không hoạt động tốt.

2.2 Brief Introduction to JPEG Baseline Encoding and Decoding

Phần này tóm tắt ngắn gọn các bước mã hóa và giải mã cơ bản của JPEG để hỗ trợ việc hiểu về phương pháp đề xuất. JPEG là một kỹ thuật nén mất mát dựa trên khối, biến đổi các khối ảnh kích thước 8x8 thành các khối hệ số DCT đã được lượng tử hóa 8x8. Quá trình biến đổi bao gồm việc chuẩn hóa bằng cách trừ 128 từ mỗi pixel, biến đổi góc dọc disket (DCT), chia cho bảng lượng hóa, thường được tỉ lệ bằng một hệ số tỉ lệ gọi là hệ số lượng tử (QF) để kiểm soát hiệu ứng của nén và chất lượng hình ảnh sau đó làm tròn được để làm cho các giá trị trở thành số nguyên.

DCT được định nghĩa như sau:

$$DCT_{u,v} = \frac{\alpha(u)\alpha(v)}{4} \sum_{i=0}^{7} \sum_{j=0}^{7} p_{i,j} \cos[\frac{(2i+1)u\pi}{16}] \cos \frac{(2j+1)v\pi}{16} \tag{2.1}$$

trong đó

$$\alpha(u) = \begin{cases} \frac{1}{\sqrt{2}} & \text{if u = 0} \\ 1 & \text{if } else \end{cases} \tag{2.2}$$

và $p_{i,j}$ đại diện cho giá trị pixel tại vị trí $(i,h), \text{Œ}CT_{u,v}$ tại vị trí (u,v).

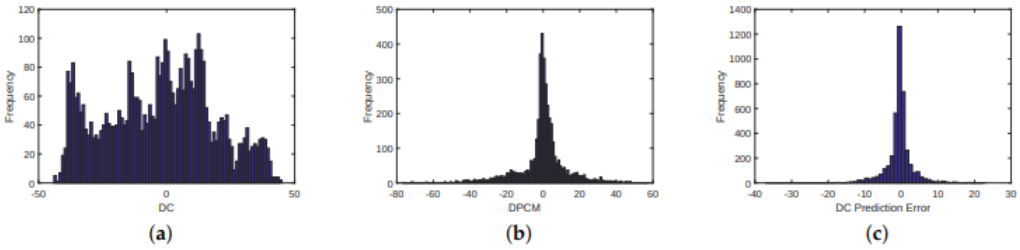
Sau khi thu được các hệ số DCT đã lượng tử hóa, chúng sẽ được nén có mất mát. Các hệ số DCT đã được lượng tử hóa bao gồm hệ số DC và hệ số AC đã được lượng tử hóa.

Hệ số DC đã được lượng tử hóa là giá trị hệ số DCT đầu tiên và biểu thị một hình thức của giá trị pixel trung bình. Còn hệ số AC đã được lượng tử hóa là phần còn lại của các hệ số DCT và biểu thị các chi tiết tinh vi của khối pixel.

Mã hoá mã xung hướng sai biệt (DPCM - differential pulse code modulation), trong đó sự khác biệt giữa hai giá trị liên tiếp được mã hoá, được sử dụng để nén các hệ số DC đã được lượng tử hóa trong hai khối liền kề. Sau đó, các giá trị DPCM được nén mất mát bằng cách sử dụng một biến thể của mã hóa Huffman. Đối với các hệ số AC đã được lượng tử hóa, sẽ tiến hành mã hóa độ dài chuỗi, sau đó mã hóa bằng cách sử dụng một biến thể của mã hóa Huffman.

Để tái tạo lại các pixel từ các hệ số DCT đã được lượng tử hóa, chúng ta nhân các hệ số DCT đã được lượng tử hóa với bảng lượng tử hóa và sau đó áp dụng biến đổi DCT ngược. Sau đó, chúng ta thêm 128 vào từng giá trị để hoàn ngược quá trình chuẩn hóa và cuối cùng, sử dụng hàm làm tròn để biến kết quả thành số nguyên.

Thông tin chi tiết hơn về việc mã hóa và giải mã JPEG có thể được tìm thấy trong tài liệu ISO. Từ đây trở đi, các hệ số DCT đã được lượng tử hóa (bao gồm cả hệ số AC và hệ số DC đã được lượng tử hóa) sẽ được ký hiệu bằng chữ đậm: DCT, AC và DC.



Hình 2.2: So sánh các biểu đồ tần số khác nhau. Biểu đồ lỗi dự đoán DC đề xuất có đỉnh cao nhất và entropi nhỏ nhất. (a) Biểu đồ tần số DC; (b) Biểu đồ tần số DPCM DC; (c) Biểu đồ lỗi dự đoán DC

2.3 Proposed Method

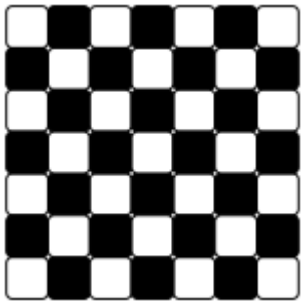
Phương pháp đề xuất sử dụng một kỹ thuật ẩn dữ liệu có khả năng đảo ngược gọi là dịch chuyển biểu đồ tần số, trong đó hiệu suất phụ thuộc mạnh vào độ chính xác của dự đoán. Việc nhúng và sự méo mó của dịch chuyển biểu đồ tần số tương quan với lỗi dự đoán; lỗi dự đoán nhỏ hơn có nghĩa là khả năng nhúng cao hơn với méo mó thấp hơn.

Các công trình trước đó không sử dụng các kỹ thuật dự đoán nâng cao trong việc ẩn dữ liệu có khả năng đảo ngược trong JPEG vì người ta nghĩ rằng việc dự đoán trong miền DCT là khá khó khăn và không đáng đối với công sức bỏ ra.

Mặc dù giả định này đúng, nhưng không đúng cho tất cả DCT. DCT đầu tiên trong khối được0 biến đổi DCT, còn được gọi là hệ số DC. Phương pháp đề xuất xây dựng trên ý tưởng này để đề xuất một phương pháp dự đoán DC, sẽ tăng khả năng nhúng và giảm méo mó.

Hình 2.2 cho thấy biểu đồ tần số của hình ảnh Lena (QF = 50). Biểu đồ tần số của DC có nhiều đỉnh và có entropi lớn nhất, biểu đồ tần số của hệ số DC dự đoán khác biệt (DPCM) tốt hơn cho dịch chuyển biểu đồ tần số so với biểu đồ DC vì nó có một đỉnh cao xung quanh 0 và entropi thấp hơn, và cuối cùng, biểu đồ tần số của biểu đồ lỗi dự đoán DC đề xuất có đỉnh cao nhất và entropi nhỏ nhất, tạo nên lựa chọn lý tưởng cho việc dịch chuyển biểu đồ tần số.

Các phần tiếp theo mô tả phương pháp dự đoán DC, phương pháp nhúng và phương pháp trích xuất.



Hình 2.3: Caption

2.3.1 DC Prediction

Trong việc dự đoán trong nén hình ảnh, chỉ có các khối giải mã có thể được sử dụng cho dự đoán, dự đoán trong ẩn dữ liệu có khả năng đảo ngược có thể sử dụng tất cả các khối không được sử dụng để nhúng. Nói cách khác, chúng ta có thể chia các khối thành hai tập không chồng chéo, tập "trắng" và tập "đen", và nhúng chúng một lần để tạo điều kiện cho việc dự đoán chính xác hơn (xem **Hình 2.3**). Không mất tính tổng quát, tập trắng được nhúng trước, sau đó tới tập đen.

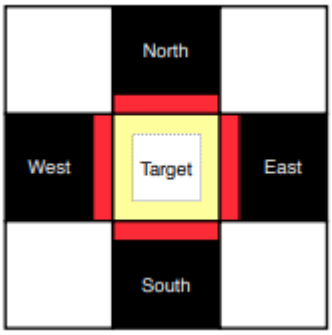
Trước khi giải thích phương pháp dự đoán đề xuất, ta định nghĩa T hoặc target block như là khối mà chúng ta muốn dự đoán hệ số DC. Hơn nữa, chỉ số trên AC được sử dụng để biểu thị rằng khối được tái xây dựng chỉ sử dụng thành phần AC.

Sau đó T^{AC} được sử dụng để biểu thị khối mục tiêu đã tái xây dựng một phần bằng cách chỉ sử dụng thành phần AC từ khối mục tiêu (giá trị DC được đặt là 0). Do DCT là một hàm tuyến tính, T có thể được phân rã gần đúng như sau:

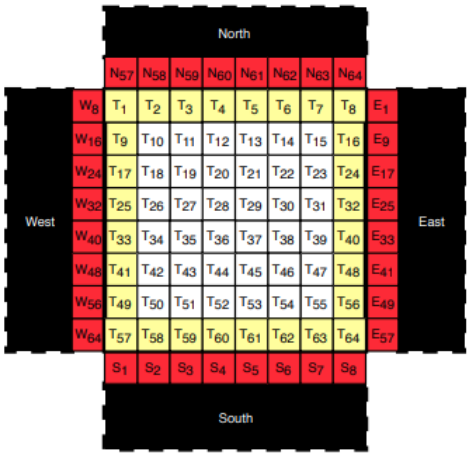
$$T \approx T^{AC} + DC \times \frac{Q_1}{8} \tag{2.3}$$

trong đó Q_1 là giá trị lượng tử hóa được sử dụng để chia hệ số DC để thu được DC, $DC \times \frac{Q_1}{8}$ biểu thị tác động của biến đổi DCT nghịch đảo lên DC.

Phương pháp dự đoán đề xuất sử dụng các khối lân cận và các khối tái xây dựng một phần bằng cách chỉ sử dụng thành phần AC. Các khối **DCT** lân cận được biến đổi thành các khối pixel của "Bắc", "Đông", "Nam" và "Tây" đầu tiên.



Hình 2.4: Ví dụ về ngữ cảnh được sử dụng cho việc dự đoán.



Hình 2.5: Ngữ cảnh được sử dụng để dự đoán DC. Giá trị pixel láng giềng từ các khối đã giải mã (Bắc, Tây, Nam và Đông), và khối mục tiêu tái xây dựng một phần T^{AC} được sử dụng để cải thiện độ chính xác dự đoán.

Hình 2.4 cho thấy góc nhìn đồ họa về sự chia tách. Khu vực màu đỏ đại diện cho các phần của các khối lân cận gần khối mục tiêu nhất, và khu vực màu vàng đại diện cho các phần của khối mục tiêu gần khối lân cận nhất.

$$Pixel_{red} \approx Pixel_{yellow} \tag{2.4}$$

Kết hợp hai phương trình 2.3 và 2.4, ta có

$$Pixel_{red} \approx Pixel^{AC}_{yellow} + DC \times \frac{Q_1}{8} \tag{2.5}$$

Rút gọn lại phương trình, ta được $\hat{DC}$: là gá trị dự đoán của **DC**

$$\hat{DC} = [\frac{8}{Q_1} \times (Pixel_{red} - Pixel^{AC}_{yellow})] \tag{2.6}$$

với [.] là hàm làm tròn số. Cuối cùng, vì có nhiều $Pixel_{red}$ và $Pixel^{AC}_{yellow}$ giá trị trung bình được sử dụng như một công cụ ước tính để đánh giá $\hat{DC}$:

$$\hat{DC} = [\frac{8}{Q_1} \times \frac{\sum_{neighbor}(Pixel_{red} - Pixel^{AC}_{yellow})}{\#ofneighhbors}] \tag{2.7}$$

$$= [\frac{8}{Q_1} \times \frac{\sum_{North,East,South,West}(Pixel_{red} - Pixel^{AC}_{yellow})}{32}] \tag{2.8}$$

$$= [\frac{8}{Q_1} \times \frac{\sum_{n=1}^{8}(N_{56+n} - T^{AC}_{n}) + (E_{8n-7} - T^{AC}_{8n}) + (S_n - T^{AC}_{n+56}) + (W_{8n} - T^{AC}_{8nn-7})}{32}] \tag{2.9}$$

2.3.2 Embedding

Kỹ thuật dịch chuyển biểu đồ tần số được sử dụng để nhúng vào các giá trị lỗi dự đoán đã được nhúng được ký hiệu bằng DC', và được thu được bằng cách sử dụng phương trình sau:

$$DC' = \begin{cases} \text{DC - b} & \text{if } DC - \hat{DC} = -1 \\ \text{DC + b} & \text{if } DC - \hat{DC} = 0 \\ \text{DC - 1} & \text{if } DC - \hat{DC} < -1 \\ \text{DC + 1} & \text{if } DC - \hat{DC} > 0 \\ DC & else \end{cases} \tag{2.10}$$

với $b \in \{0,1\}$ là payload bit.

Kỹ thuật dịch chuyển biểu đồ tần số di chuyển DC với các sai số dự đoán nhỏ hơn -1 bằng -1, để có thể nhúng DC có giá trị -1 bằng cách sử dụng hệ số có giá trị -1 và -2: hệ số có giá trị -1 sẽ được thay đổi thành -2 nếu bit dữ liệu là "1", và giữ nguyên -1 nếu bit dữ liệu là "0". Logic tương tự áp dụng cho DC với sai số dự đoán lớn hơn 0. Vì kỹ thuật dịch chuyển biểu đồ tần số được áp dụng

sao cho chúng không giao nhau, nên nó có thể được đảo ngược. Phần tiếp theo sẽ thảo luận về việc trích xuất dữ liệu và khôi phục lại DC ban đầu.

2.3.3 Extraction and Recovery

Việc trích xuất dữ liệu và khôi phục lại DC ban đầu là khá đơn giản.

$$b = \begin{cases} 0 & \text{if DC' = -1} \\ 0 & \text{if DC' = 0} \\ 1 & \text{if DC' = -2} \\ 1 & \text{if DC' = 1} \end{cases} \tag{2.11}$$

$$DC = \begin{cases} \text{DC' + 1} & \text{if } DC' - \hat{DC} < 1 \\ \text{DC' - 1} & \text{if } DC' - \hat{DC} > 0 \\ \text{DC'} & \text{if } else \end{cases} \tag{2.12}$$

2.4 Block Selection

Việc lựa chọn khối là quan trọng trong các trường hợp không sử dụng hết khả năng nhúng đầy đủ. Để ảnh hưởng nhỏ nhất đến PSNR, các khối được sắp xếp theo độ mịn của chúng và các khối được nhúng tuần tự chỉ đến khi tất cả dữ liệu đã được nhúng.

Để đảm bảo rằng các khối mịn nhất được nhúng trước, thuật toán lựa chọn khối được đề xuất bởi Huang et al. được sử dụng. Trong thuật toán này, số lượng hệ số DCT bằng 0 được sử dụng như một đại lượng đo độ mịn để sắp xếp các khối. Giả định ở đây là các khối DCT với nhiều hệ số DCT bằng không sẽ có ít chi tiết hơn và do đó mịn hơn.

Trong phương pháp đề xuất, hệ số DCT bằng 0 không được sử dụng để đo độ mịn và chỉ các hệ số DCTbằng 0 được sử dụng để đo độ mịn. Hệ số DCT không được sử dụng vì chúng có thể thay đổi sau khi nhúng.

2.5 Encoder and Decoder

Phần này tóm tắt phương pháp mã hóa và giải mã của việc ẩn dữ liệu đảo ngược được đề xuất. Mỗi phần nhỏ sẽ mô tả các bước thực hiện và bao gồm các chi tiết thực hiện nhỏ để giúp hiểu rõ hơn.

2.5.1 Encoder

1. Trích xuất các khối DCT từ hình ảnh JPEG.
2. Chia các khối thành tập trắng và tập đen.
3. Sử dụng phương pháp lựa chọn khối để sắp xếp tập trắng của DC
4. Dự đoán tập trắng của DC và nhúng nửa lượng dữ liệu nhúng.
5. Sử dụng phương pháp lựa chọn khối để sắp xếp tập đen của DC.
6. Dự đoán tập đen của DC và nhúng phần còn lại của dữ liệu nhúng bao gồm độ dài của dữ liệu nhúng, được thêm vào phía trước phần còn lại của dữ liệu nhúng. (Dự đoán sử dụng DC' đã được nhúng từ bước 4.)

2.5.2 Decoder

1. Trích xuất các khối DCT đã được nhúng từ hình ảnh JPEG.
2. Chia các khối thành tập trắng và tập đen.
3. Sử dụng phương pháp lựa chọn khối để sắp xếp tập đen của DC'.
4. Dự đoán tập đen của DC', trích xuất độ dài của dữ liệu nhúng và nửa phần của dữ liệu nhúng, và khôi phục lại DC ban đầu cho tập đen.
5. Sử dụng phương pháp lựa chọn khối để sắp xếp tập trắng của DC.
6. Dự đoán tập trắng của DC', trích xuất nửa đầu của dữ liệu nhúng, và khôi phục lại DC ban đầu cho tập trắng. (Dự đoán sử dụng DC ban đầu đã khôi phục từ bước 4.)

2.6 Experiment

Hiệu suất của phương pháp đề xuất được xác minh bằng cách sử dụng so sánh PSNR (giữa hình ảnh JPEG gốc và hình ảnh JPEG đã nhúng) và so sánh ưu điểm về kích thước tệp (do quá trình nhúng) của các phương pháp. Tuy nhiên, không có công trình nào hiện có tập trung vào việc nhúng trong DC. Do đó, một biến thể của phương pháp của Huang et al., là thuật toán tiên tiến nhất về PSNR và lợi ích về kích thước tệp, được so sánh với phương pháp đề xuất.

Các giá trị của hệ số lượng tử hóa (QF) 50 và 80 được chọn để so sánh. Bảng lượng tử hóa dựa trên QF =50 là bảng lượng tử hóa cơ sở được khuyến nghị viết trong tài liệu tiêu chuẩn, được tỷ lệ để thu được bảng lượng tử hóa khác, là một bộ tiêu chuẩn tốt để kiểm tra. Bảng lượng tử hóa dựa trên QF =80 là bảng được biết đến là đạt được tỷ lệ nén tốt.

Tài liệu tham khảo

[1] Zhengjun Liu et al. “Image watermarking by using phase retrieval algorithm in gyrator transform domain”. In: *Optics Communications* 283.24 (2010), pp. 4923–4927.

[2] Mansi S Subhedar and Vijay H Mankar. “Current status and key issues in image steganography: A survey”. In: *Computer science review* 13 (2014), pp. 95–113.

[3] Suah Kim, Fangjun Huang, and Hyoung Joong Kim. “Reversible data hiding in JPEG images using quantized DC”. In: *Entropy* 21.9 (2019), p. 835.

[4] Chanil Pak et al. “A novel color image LSB steganography using improved 1D chaotic map”. In: *Multimedia Tools and Applications* 79.1-2 (2020), pp. 1409–1425.