PHƯƠNG PHÁP MẬT MÃ HÓA ẢNH MÀU RGB SỬ DỤNG PHÉP NHÂN MA TRẬN

Đỗ Đình Hưng[1*], Vương Hoàng Nam[2]
[*]Tác giả liên hệ, Email: hungdd@hou.edu.vn

Ngày tòa soạn nhận được bài báo: 02/06/2025
Ngày phản biện đánh giá: 08/09/2025
Ngày bài báo được duyệt đăng: 15/10/2025

DOI: 10.59266/houjs.2025.724

Tóm tắt: *Trong bài báo này các tác giả trình bày sự cần thiết của việc cải tiến các kỹ thuật mã và giải mã ảnh màu RGB về thời gian cũng như tính năng bảo mật. Nội dung chính của bài báo là đề xuất một kỹ thuật mã hóa tiên tiến sử dụng các ảnh thành phần R, G, B của ảnh màu RGB để áp dụng phép toán nhân ma trận và ma trận nghịch đảo nhằm thực hiện mã hóa và giải mã ảnh màu thông qua quá trình xây dựng một thuật toán mật mã hóa mới hiệu quả.*

Kết quả mô phỏng mà thuật toán đề xuất đã minh chứng sự hiệu quả do phương pháp này đem lại so với một số phương pháp mã hóa và giải mã ảnh màu đã được phát triển. Thuật toán này đã tối ưu hóa thời gian mã - giải mã so với một vài phương pháp mã hóa đã được đề xuất trước đó.

Từ khóa: *ảnh màu RGB, mật mã hóa, giải mật mã hóa, nhân ma trận (matrix), thuật toán Al-Laham*

I. Đặt vấn đề

Hiện nay, giới khoa học đang chứng kiến sự phát triển nhanh và phổ biến của các ứng dụng về đa phương tiện, việc trao đổi và truyền tải dữ liệu hình ảnh, video qua mạng công cộng ngày càng phổ biến hơn. Tuy nhiên, điều này cũng đưa đến sự gia tăng đáng kể các sự cố về bảo mật đặc biệt là hành vi tấn công nhằm đánh cắp, thao túng hoặc làm giả dữ liệu đa phương tiện.

Do vậy, mặc dù có nhiều thuật toán về mã hóa ảnh đã được đề xuất, nhưng vẫn tồn tại khoảng cách không nhỏ giữa

[1] Khoa Điện - Điện Tử, Trường Đại học Mở Hà Nội
[2] Đại học Bách Khoa Hà Nội

yêu cầu về bảo mật và hiệu suất xử lý. Một số thuật toán tuy có khả năng xử lý cao, hoàn toàn có thể đáp ứng được yêu cầu về thời gian thực, nhưng lại chỉ đảm bảo mức độ bảo mật hạn chế. Ngược lại, các thuật toán có mức độ bảo mật cao thường gặp phải vấn đề về hiệu suất, khiến cho việc áp dụng trong các hệ thống đòi hỏi xử lý nhanh và liên tục trở nên khó khăn [4-7].

Bên cạnh đó, nhiều thuật toán hiện tại còn chứa các thao tác dư thừa hoặc sử dụng các phương pháp tìm kiếm tốn kém về mặt tính toán, gây ảnh hưởng tiêu cực đến thời gian xử lý dữ liệu và khả năng có thể mở rộng đối với các ứng dụng thực tế. Điều này tạo ra thách thức lớn trong việc phát triển giải pháp mã hóa ảnh vừa đảm bảo an toàn dữ liệu, đồng thời đáp ứng được yêu cầu về hiệu suất trong môi trường đa phương tiện ngày càng phức tạp [8].

Một thuật toán mã hóa ảnh màu hiệu quả đã được đề xuất bởi Al-Laham (2015) [2] và Al-Laham et al. (2016) [3]. Thuật toán này đã sử dụng một phép nhân ma trận để tiến hành việc mã và giải mã ảnh màu.

Nội dung nghiên cứu trong bài báo là đề xuất một kỹ thuật mới được các tác giả phát triển lên dựa trên thuật toán của Al-Laham nhằm cải thiện chất lượng mã hóa - giải mã ảnh màu. Các đóng góp chủ yếu của bài báo bao gồm:

- Xây dựng một thuật toán mã và giải mã ảnh màu mới, sử dụng 1 phép nhân ma trận kết hợp với ma trận nghịch đảo trong quá trình mã hóa - giải mã ảnh màu RGB tương tự thuật toán Al-Laham [2].

- Đề xuất các kỹ thuật mới nhằm giảm thiểu thời gian mã hóa – giải mã ảnh màu. Kết quả thực nghiệm được so sánh với phương pháp mã hóa ảnh RGB sử dụng ảnh xám đề xuất bởi Ahmad A.M. Sharadqah. (2015) [1] và thuật toán mật mã hóa ảnh màu đề xuất bởi Al-Laham [2].

II. Phương pháp đề xuất

Thuật toán được tác giả đề xuất dựa trên việc chuyển đổi hình ảnh màu ba chiều (RGB) ban đầu thành ma trận 2 chiều. Cụ thể, ma trận hai chiều này được mã hóa trực tiếp bằng phương pháp đề xuất mà không yêu cầu thêm bước chuyển đổi, đồng thời áp dụng các kỹ thuật hoán vị và thay thế lên ma trận đó.

Quá trình mã hóa được đề xuất bao gồm chuỗi các bước như sau:

Bước 1: Chuyển đổi hình ảnh màu LxW điểm ảnh, gồm 3 thành phần (RGB) có kích thước (L×W×3) thành ma trận hai chiều (3L×W).

Bước 2: Tạo khóa ma trận vuông ngẫu nhiên (EK-ma trận mã hóa) với kích thước (W×W).

Bước 3: Tạo hai khóa vectơ ngẫu nhiên (RK1) và (RK2) (kích thước 1x 3L) với các giá trị thay đổi ngẫu nhiên không bị trùng lặp từ 1 đến 3L.

Bước 4: Tạo hai khóa vectơ ngẫu nhiên (CK1) và (CK2) (kích thước 1 x W) với các giá trị thay đổi ngẫu nhiên không bị trùng lặp từ 1 đến W.

Bước 5: Thay đổi thứ tự hàng của ma trận hai chiều theo khóa RK1.

Bước 6: Thay đổi thứ tự cột của ma trận kết quả ở bước 5 theo khóa CK1.

Bước 7: Nhân ma trận hai chiều với khóa EK.

Bước 8: Thay đổi thứ tự hàng của ma trận kết quả ở bước 7 theo khóa RK2.

Bước 9: Thay đổi thứ tự cột của ma trận kết quả ở bước 8 theo khóa CK2.

Bước 10: Định hình lại ma trận hai chiều thành ma trận ba chiều có kích thước (L×W×3).

Trong thuật toán đề xuất, trước khi nhân với khóa ma trận EK (tương tự thuật toán của Al Laham 2015), thông tin cần mã hóa (ma trận hai chiều 3LxW) sẽ được đảo thứ tự vị trí các hàng và cột theo giá trị các khóa RK1 và CK1. Sau khi nhân với khóa ma trận , thông tin đã mã hóa lại tiếp tục đảo vị trí các hàng và cột giá trị của khóa RK2 và CK2. Điều đó dẫn đến thông tin sau mật mã hóa đã được bảo mật hơn.

Quá trình giải mã, gồm chuỗi các bước sau:

Bước 1: Chuyển đổi hình ảnh ba chiều được mã hóa có kích thước (L×W×3) sang ma trận hai chiều (3L×W).

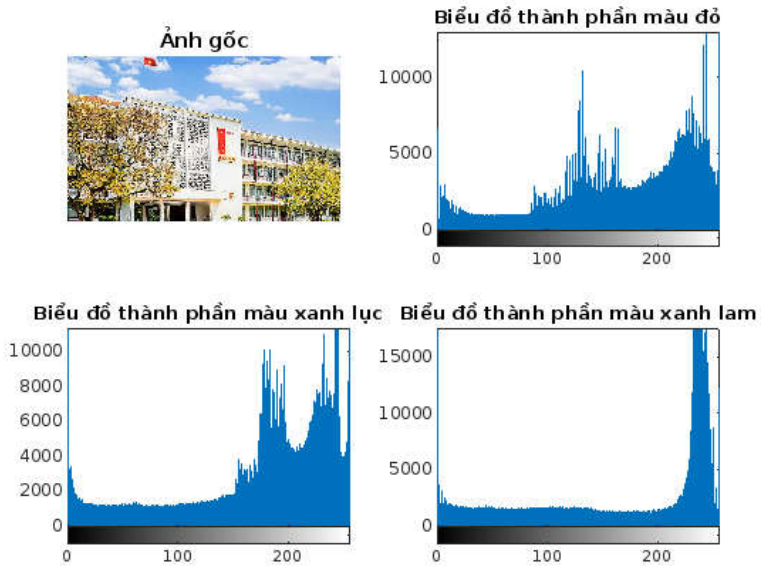
Bước 2: Thay đổi thứ tự cột và hàng của hình ảnh được mã hóa theo khóa CK2 và RK2.

Bước 3: Nhân ma trận kết quả ở bước 1 với ma trận nghịch đảo EK.

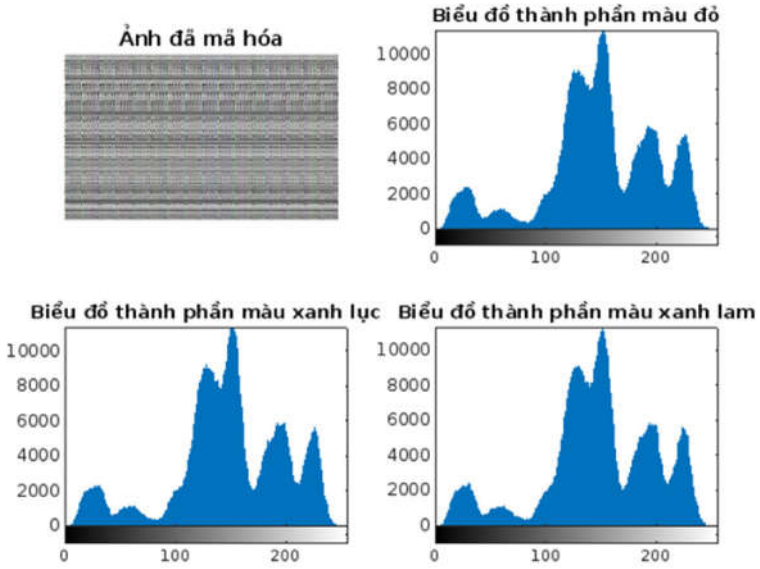
Bước 4: Thay đổi thứ tự cột và hàng của ma trận kết quả ở bước 2 theo các khóa CK1 và RK1.

Bước 5: Định hình lại ma trận hai chiều thành hình ảnh màu ba chiều (RGB).

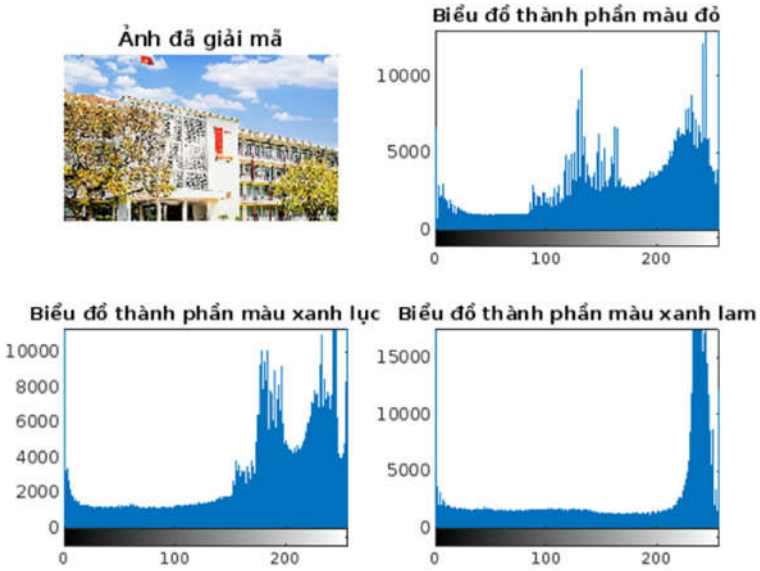
Hình 2.1, 2.2 và 2.3 là một minh họa kết quả mã hóa và giải mã ảnh bằng phương pháp đề xuất.



Hình 2.1. Hình ảnh gốc 214×235×3 và biểu đồ histogram thành phần



Hình 2.2. Ảnh mã hóa và histogram



Hình 2.3. Ảnh giải mã và histogram

III. Kết quả và thảo luận định hướng

Trong phần trình bày này, hiệu quả của kỹ thuật mật mã hóa ảnh màu được phát triển sẽ được chứng minh rõ ràng. Trên thực tế, các phương pháp mật mã được đề cập trong bài báo không có sự khác biệt nhiều về chất lượng ảnh sau khi giải mã. Do đó, thời gian cần thiết đối với quá trình mã hóa và giải mã ảnh màu đã được so sánh với phương pháp do Sharadqa (2015) [1] và Al-Laham (2015) [2] đề xuất. Phân tích thời gian được thực hiện bằng máy tính xách tay với bộ vi xử lý Intel Core i9 với tốc độ 2.8 GHz và bộ nhớ trong RAM 8 GB, trong khi việc triển khai thuật toán

sử dụng phần mềm MATLAB 2013, một công cụ mạnh mẽ chuyên biệt cho thiết kế và xử lý ma trận. Kết quả cho thấy kỹ thuật tác giả đề xuất vượt trội hơn so với phương pháp của Sharadqa.

Ngoài ra, kết quả của thuật toán cũng được đánh giá chi tiết và so sánh với cả phương pháp của Sharadqa và của Al-Laham dựa trên thu thập từ nhiều ảnh màu có kích thước khác nhau.

Phương pháp của Sharadqa (2015) [1] dựa trên việc chuyển đổi ảnh màu sang ảnh xám trước khi thực hiện mã hóa. Tuy nhiên, theo nghiên cứu của Al-Laham (2015) [2], phương pháp này vẫn tồn tại một vài hạn chế đáng kể như:

• Yêu cầu thêm bộ nhớ lưu trữ do cần tách ảnh thành các thành phần R,G và B riêng biệt.

• Tiêu tốn nhiều thời gian vì phải xử lý từng thành phần màu một cách độc lập, như đã đề cập ở trên.

Bảng 3.1 và 3.2 trình bày kết quả đo lường thời gian mã hóa - giải mã cùng kích thước khóa mã hóa của các phương pháp áp dụng trên nhiều ảnh màu khác nhau. Kết quả thu được cho chúng ta thấy kỹ thuật đề xuất không chỉ giảm đáng kể thời gian xử lý so với phương pháp của Sharadqa mà còn tối ưu hóa kích thước khóa vượt trội hơn thuật toán Al-Laham [2]. Điều này khẳng định hiệu quả cao và tiềm năng ứng dụng thực tiễn của phương pháp đề xuất.

Bảng 3.1: Thời gian mã hóavà giải mã cho kỹ thuật được đề xuất

Kích thước hình ảnh	**Tổng thời gian mã hóa và giải mã của thuật toán đề xuất (giây)**	**Tổng thời gian mã hóa và giải mã của thuật toán [2] (giây)**	**Tổng thời gian mã hóa và giải mã của thuật toán [1] (giây)**
183*276*3	0.012278	0.021477	0.030756
164*308*3	0.014549	0.022794	0.033343
186*270*3	0.012806	0.01932	0.030126
225*225*3	0.008289	0.01729	0.027579
214*235*3	0.008568	0.016683	0.028251
333*360*3	0.019525	0.043181	0.052703
183*275*3	0.011713	0.019085	0.031794
300*400*3	0.023308	0.046425	0.079733
198*255*3	0.011813	0.01794	0.029951
160*160*3	0.006332	0.007333	0.013961
194*259*3	0.012845	0.017884	0.032724

Bảng 3.2: So sánh kích thước khóa giữa phương pháp tác giả đề xuất và phương pháp được đề xuất bởi (Sharadqah, 2015) và (Al-Laham, 2015).

Kích thước hình ảnh	**Kích thước khóa mã hóa/giải mã đề xuất bởi (Al-Laham, 2015)**	**Kích thước khóa mã hóa/giải mã đề xuất bởi (Sharadqah, 2015)**	**Kích thước khóa mã hóa /giải mã của phương pháp đề xuất**
183*276*3	390*390	276*276	(276*279)+183
164*308*3	390*390	308*308	(308*311)+164

Kích thước hình ảnh	Kích thước khóa mã hóa/giải mã đề xuất bởi (Al-Laham, 2015)	Kích thước khóa mã hóa/giải mã đề xuất bởi (Sharadqah, 2015)	Kích thước khóa mã hóa /giải mã của phương pháp đề xuất
186*270*3	389*389	270*270	(270*273)+186
225*225*3	390*390	225*225	(225*228)+225
214*235*3	389*389	235*235	(235*238)+214
333*360*3	600*600	360*360	(360*363)+333
183*275*3	389*389	275*275	(275*278)+183
300*400*3	600*600	400*400	(400*403)+300
198*255*3	390*390	255*255	(255*258)+198
160*160*3	278*278	160*160	160*164
194*259*3	389*389	259*259	(259*262)+194

IV. Kết luận

Bài báo này đã được tác giả đưa ra một phương pháp mật mã hóa ảnh màu sử dụng phép nhân ma trận. Thuật toán được đề xuất là cải tiến của thuật toán Al-Laham (2015) [2]. Kết quả mô phỏng của thuật toán đề xuất đã chứng minh tính hiệu quả của thuật toán so với một số phương pháp mật mã hóa và giải mã ảnh màu đã được công bố. Thuật toán này đã tối ưu thời gian mã hóa - giải mã so với một số phương pháp mã hóa đã được đề xuất trước đó.

Tài liệu tham khảo:

[1]. Sharadqah, A. A. M. (2015). RGB colored image encryption-decryption using gray image. *International Journal of Computer Science Issues (IJCSI), 12*(3), 1694–0784.

[2]. Al-Laham, M. (2015). Encryption-decryption RGB color image using matrix multiplication. *International Journal of Computer Science & Information Technology (IJCSIT), 7*(4), 45–52. https://doi.org/10.5121/ijcsit.2015.7404

[3]. Rasmi, M., Al-Salameen, F., Al-Laham, M. M., & Al-Fayomi, A. (2016). Enhancing RGB color image encryption-decryption using one-dimensional matrix. In *Proceedings of the International Arab Conference on Information Technology (ACIT'2016)* (pp. 1–6).

[4]. Ayushi, M. (2011). A symmetric key cryptographic algorithm. *International Journal of Computer Applications, 1*(15), 1–6. https://doi.org/10.5120/331-502

[5]. Santhi, B., Ravichandran, K. S., Arun, A. P., & Chakkarapani, L. (2012). A novel cryptographic key generation method using image features. *Journal of Information Technology, 4*(2), 88–92. ISSN: 2041-3114.

[6]. Xie, R., Wang, M., & Hai, B. (2015). Image encryption research based on key extracted from iris feature. *International Journal of Security and Its Applications (IJSIA), 9*(6), 157–166.

[7]. Gedam, M. T. (2014). Image encryption technique based on visual cryptography. *International Journal of Research (IJR), 11*(1), 22–26. ISSN: 2348-6848.

[8]. Kang, W. (2024). Multidimensional image encryption and decryption technology. *Journal of the Franklin Institute, 361*(18), 107315. https://doi.org/10.1016/j.jfranklin.2024.107315

A ENCRYPTION METHOD FOR RGB COLOR IMAGE USING MATRIX MULTIPLICATION

Do Dinh Hung[3], Vuong Hoang Nam[4]

Abstract: *This study explores the integration of AI in programming education to deliver personalized learning tools tailored to each student's needs and pace. Platforms such as GitHub Copilot, Tabnine, and CodiumAI have shown effectiveness in improving programming skills, boosting motivation, and making C++ learning more accessible through instant feedback, gamification, and adaptive study plans. AI also streamlines learning by reducing repetitive tasks, allowing instructors to focus on higher-level guidance. However, challenges persist regarding data privacy, algorithmic bias, and striking a balance between AI assistance and the development of critical thinking.*

Keywords: *RGB - color image, encryption, decryption, matrix - multiplication, Al-Laham algorithm*

[3] Faculty of Electrical and Electronics Engineering, Hanoi Open University
[4] Hanoi University of Science and Technology