

NÉN ẢNH Y SINH 3D VÀ BẢO MẬT THÔNG TIN CÁ NHÂN

Nguyễn Lương Nhật

Học viện Công nghệ Bưu chính Viễn thông

Tóm tắt: Bài báo này đề xuất một hệ thống truyền tin mật kết hợp các thuật toán nén, mã hóa và giấu tin, mục đích là đưa ra một giải pháp truyền tin mới đảm bảo sự an toàn cho thông tin cá nhân nhạy cảm, hiệu quả trong lưu trữ và truyền tin, đồng thời vẫn giữ được các đặc trưng cần thiết của ảnh y sinh 3D (Three-dimensional). Ảnh y sinh ban đầu sẽ được nén bằng phương pháp phân tích wavelet 3D trước khi thông tin cá nhân được nhúng vào dùng kỹ thuật giấu tin thuận nghịch. Thông tin cá nhân và ảnh y sinh trước khi nhúng sẽ được khôi phục hoàn toàn chính xác tại phía thu, ngoài ra thuật toán mã hóa AES (Advanced Encryption Standard) giúp tăng tính bảo mật của thông tin cá nhân.

Từ khóa: 3D compression, 3D DWT, Patient confidentiality, Reversible data hiding.

I. GIỚI THIỆU

Quá trình trao đổi hình ảnh y tế qua internet đã thu hút sự quan tâm đáng kể của các nhà khoa học trong vài năm qua do sự ra đời của thông tin y tế dựa trên web và các hệ thống đám mây. Những dữ liệu y sinh như điện tim, trị số đường, huyết áp, ... cùng với các thông tin cá nhân quan trọng khác của bệnh nhân được truyền qua các kênh không an toàn và lưu trữ trong cơ sở hạ tầng đám mây [1], [2], [3]. Trong quá trình truyền và lưu trữ, việc rò rỉ dữ liệu riêng tư này có nhiều rủi ro hơn bao giờ hết nên việc bảo vệ dữ liệu nhạy cảm luôn là một chỉ số quan trọng để đánh giá hiệu suất của các hệ thống.

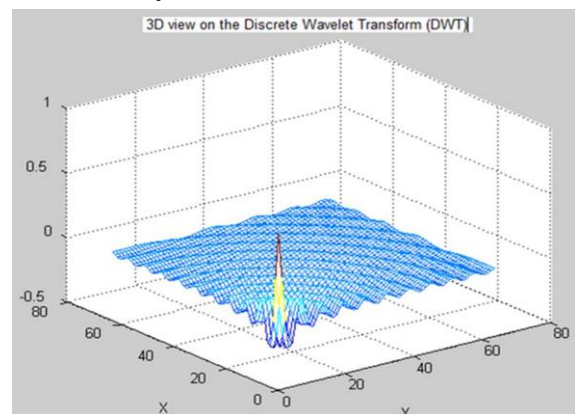
Trong [4], [5] các tác giả đã đề xuất nhúng thông tin bệnh nhân vào dữ liệu điện tâm đồ để đảm bảo an toàn cho thông tin cá nhân của bệnh nhân. Sau đó, các tác giả của [6] trình bày một phương pháp nhúng thông tin vào tín hiệu điện tim kết hợp với nén dữ liệu. Khuyết điểm chung của các phương pháp trên là dữ liệu y sinh chứa thông tin không thể khôi phục chính xác về trạng thái gốc như trước khi nhúng thông tin.

Với ngữ cảnh đó, bài báo trình bày một phương pháp bảo mật thông tin cá nhân như: thông tin bệnh nhân, thông tin thuốc, ghi chú của bác sĩ, ... sử dụng kỹ thuật giấu tin trong ảnh y sinh 3D, kết hợp với thuật toán mã hóa tiên tiến AES (Advanced Encryption Standard) để tăng tính bảo mật cho dữ liệu. Quá trình nhúng sử dụng kỹ thuật giấu tin thuận nghịch đảm bảo khôi phục hoàn toàn ảnh y sinh gốc. Đồng thời để thuận lợi cho việc lưu trữ và truyền dẫn, thuật toán nén ảnh y sinh 3D được áp dụng

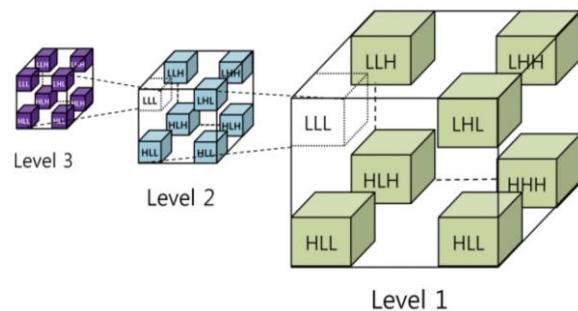
trước khi nhúng nhằm giảm đi đáng kể dung lượng của dữ liệu y sinh.

Trong phần II bài báo sẽ mô tả về kỹ thuật nén ảnh y sinh 3D dựa trên phân giải wavelet 3D, phần III trình bày thuật toán giấu tin thuận nghịch áp dụng cho ảnh y sinh. Phần IV trình bày mô hình hệ thống truyền tin đề xuất kết hợp kỹ thuật nén, mã hóa và giấu tin. Phần V là các kết quả thí nghiệm và phần 0 là kết luận.

II. KỸ THUẬT NÉN ẢNH Y SINH 3D



Hình 1. Chế độ xem 3D về năng lượng của DWT



Hình 2. Quá trình phân tích 3D DWT 3 mức

Ngày nay phép biến đổi wavelet đã đi đầu không chỉ trong lĩnh vực xử lý hình ảnh mà còn trong các kỹ thuật nén tín hiệu do có khả năng tập trung năng lượng cao [7], [8], [9]. Chế độ xem 3D về khả năng tập trung năng lượng của biến đổi wavelet được thể hiện như hình 1.

Kỹ thuật phân rã dữ liệu 3D wavelet dựa trên việc sử dụng kỹ thuật biến đổi 1-D trên 3 trục dữ liệu theo x , y , z . Dữ liệu 3D được sắp xếp tuần tự theo từng khung. Mỗi khung dữ liệu bao gồm các dòng và cột 2D: x , y ; được xem là hệ trục của mỗi khung ảnh, z là hệ trục các khung ảnh được sắp xếp theo tuần tự trước sau trong chuỗi những khung ảnh. Dữ liệu đầu vào là một tập các khung ảnh trong đó mỗi khung ảnh bao gồm N hàng và M cột.

Tác giả liên hệ: Nguyễn Lương Nhật,

Email: nhatnl@ptithcm.edu.vn

Đến tòa soạn: 11/2022, chỉnh sửa: 1/2023, chấp nhận đăng: 2/2023.

Theo đó, các tập dữ liệu có kích thước $N \times M \times L$, trong đó N, M, L là các số nguyên. Kỹ thuật 3D-DWT có thể được xem như là sự tích hợp của 3 bộ biến đổi 1D-DWT theo 3 chiều x, y, z , mỗi bộ biến đổi sẽ gồm các cặp bộ lọc thông cao và thông thấp biến đổi mỗi tương quan của hệ số các bộ lọc và các điểm ảnh đầu vào. Sau bước biến đổi 3D-DWT, khối dữ liệu ảnh được phân rã thành HHH, HHL, HLH, HLL, LHH, LHL, LLH, LLL như hình 2.

Cơ sở toán học của 3D DWT được mô tả như trong [8]. Theo đó:

$$LLL = \phi(x, y, z) = \phi(x) \phi(y) \phi(z) \quad (1)$$

$$LLH = \psi^1(x, y, z) = \phi(x) \phi(y) \psi(z) \quad (2)$$

$$LHL = \psi^2(x, y, z) = \phi(x) \psi(y) \phi(z) \quad (3)$$

$$LHH = \psi^3(x, y, z) = \phi(x) \psi(y) \psi(z) \quad (4)$$

$$HLL = \psi^4(x, y, z) = \psi(x) \phi(y) \phi(z) \quad (5)$$

$$HLH = \psi^5(x, y, z) = \psi(x) \phi(y) \psi(z) \quad (6)$$

$$HHL = \psi^6(x, y, z) = \psi(x) \psi(y) \phi(z) \quad (7)$$

$$HHH = \psi^7(x, y, z) = \psi(x) \psi(y) \psi(z) \quad (8)$$

Với $i \in \{H, V, D\}$ theo 3 chiều không gian và:

$$\phi_{j,m,n,l}(x, y, z) = 2^{j/2} \phi(2^j x - m, 2^j y - n, 2^j z - l) \quad (9)$$

$$\psi_{j,m,n,l}(x, y, z) = 2^{j/2} \psi(2^j x - m, 2^j y - n, 2^j z - l) \quad (10)$$

Hàm biến đổi wavelet rời rạc $f(x, y, z)$ của khối dữ liệu 3 chiều $M \times N \times L$ được trình bày như sau:

Hàm chia tỉ lệ biểu diễn bởi:

$$W_\phi(j_0, m, n, l) = \frac{1}{\sqrt{MNL}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \sum_{z=0}^{L-1} f(x, y, z) \phi_{j_0, m, n, l}(x, y, z) \quad (11)$$

Hàm băng con theo các chiều không gian được mô tả lần lượt bởi:

$$W_\psi^H(j, m, n, l) = \frac{1}{\sqrt{MNL}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \sum_{z=0}^{L-1} f(x, y, z) \psi_{j, m, n, l}^H(x, y, z) \quad (12)$$

$$W_\psi^V(j, m, n, l) = \frac{1}{\sqrt{MNL}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \sum_{z=0}^{L-1} f(x, y, z) \psi_{j, m, n, l}^V(x, y, z) \quad (13)$$

$$W_\psi^D(j, m, n, l) = \frac{1}{\sqrt{MNL}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \sum_{z=0}^{L-1} f(x, y, z) \psi_{j, m, n, l}^D(x, y, z) \quad (14)$$

Từ W_ψ và W_ϕ ta có thể dễ dàng có được biến đổi rời rạc ngược của khối dữ liệu 3D như sau:

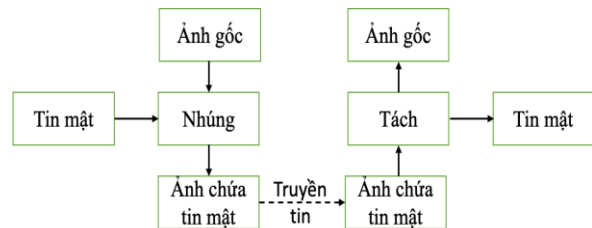
$$f(x, y, z) = \frac{1}{\sqrt{MNL}} \sum_{i=H,V,D} \sum_{j=j_0}^{\infty} \sum_m \sum_n \sum_l W_\psi^i(j, m, n, l) \psi_{j, m, n, l}^i(x, y, z) + \frac{1}{\sqrt{MNL}} \sum_m \sum_n \sum_l W_\phi(j_0, m, n, l) \phi_{j_0, m, n, l}(x, y, z) \quad (15)$$

Như đã trình bày ở trên, năng lượng của khối ảnh 3D chủ yếu tập trung tại vùng tần số thấp (LLL), kỹ thuật nén ảnh 3D thực chất là giữ lại băng con này và loại bỏ các băng con khác. Giả sử ảnh gốc có giá trị mức xám đỉnh là X_{max} và khối ảnh LLL có giá trị mức xám đỉnh là Y_{max} , ảnh nén $Y'_{(x,y,z)}$ được cho bởi (16) với $Y_{(x,y,z)}$ là giá trị mức xám của khối LLL tại vị trí x, y, z .

$$Y'_{(x,y,z)} = \frac{Y_{(x,y,z)} \cdot X_{max}}{Y_{max}} \quad (16)$$

III. GIẤU TIN THUẬN NGHỊCH

Giấu tin là kỹ thuật ẩn các dữ liệu nhạy cảm bên trong các phương tiện chứa khác mà không gây ra quá nhiều sự thay đổi trên đối tượng chứa tin. Các kỹ thuật giấu tin thường được thiết kế để đảm bảo an toàn cho thông tin ẩn với sự biến dạng tối thiểu của tín hiệu chủ và thường được đánh giá qua các tiêu chí: tính vô hình của thông tin ẩn giấu, tính toàn vẹn dữ liệu và tính bảo mật. Ngoài ra để có thể ứng dụng cho các hệ thống y tế và quân sự, kỹ thuật giấu tin còn phải đảm bảo tính thuận nghịch (có thể đảo ngược).



Hình 3. Giấu tin thuận nghịch

Kỹ thuật giấu tin thuận nghịch đang được quan tâm nhiều hơn trong những năm gần đây vì nó cho phép khôi phục hoàn toàn chính xác dữ liệu nhúng cũng như đối tượng chứa tin [10], [11], [12]. Điều này thật sự cần thiết trong một số ứng dụng về viễn thám, xử lý hình ảnh y tế và thông tin liên lạc quân sự. Một lược đồ giấu tin thuận nghịch được biết đến như mô tả trên hình 3. Theo đó, ảnh gốc sau khi đã nhúng thông tin mật có thể được khôi phục hoàn toàn tại đầu thu sau khi các thông tin mật được trích xuất.

Xét đối tượng chứa tin là một ảnh X với thang độ xám 8 bit. Thuật toán giấu tin thuận nghịch đề xuất được thực hiện như sau:

Bước 1: Quét hình ảnh theo chiều từ trái sang phải và từ trên xuống dưới, tính toán giá trị khác biệt d_i giữa các điểm ảnh liên kề x_i và x_{i-1} của X .

$$d_i = \begin{cases} x_i, & \text{if } i=0 \\ |x_{i-1} - x_i|, & \text{khác} \end{cases} \quad (17)$$

Bước 2: Xác định P từ các giá trị khác biệt d_i (P chính là giá trị d_i có số lần xuất hiện cao nhất).

Bước 3: Các bit thông tin mật b [0, 1] sẽ được nhúng lần lượt vào ảnh X theo (18) để tạo thành ảnh đã nhúng Y .

$$y_i = \begin{cases} x_i, & \text{if } (i=0) \vee (d_i < P) \\ x_i + 1, & \text{if } (d_i > P) \ \& \& (x_i \geq x_{i-1}) \\ x_i - 1, & \text{if } (d_i > P) \ \& \& (x_i < x_{i-1}) \\ x_i + b, & \text{if } (d_i = P) \ \& \& (x_i \geq x_{i-1}) \\ x_i - b, & \text{if } (d_i = P) \ \& \& (x_i < x_{i-1}) \end{cases} \quad (18)$$

Với y_i là các các điểm ảnh tương ứng của ảnh đã nhúng Y . Sau khi nhúng thông tin mật, tại đầu thu ảnh Y cũng sẽ được quét theo chiều tương tự như đầu phát. Các bit thông tin mật b và các pixel x_i của ảnh gốc X được khôi phục chính xác theo (19) và (20).

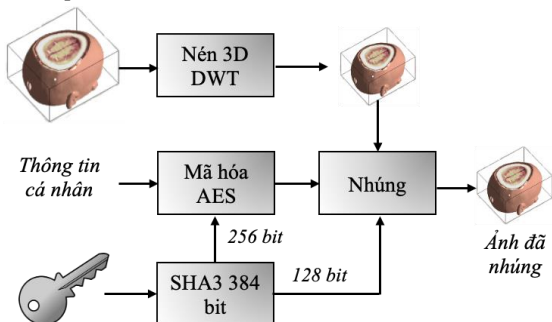
$$b = \begin{cases} 0, & \text{if } |y_i - x_{i-1}| = P \\ 1 & \text{if } |y_i - x_{i-1}| = P + 1 \end{cases} \quad (19)$$

$$x_i = \begin{cases} y_i + 1, & \text{if } |y_i - x_{i-1}| > P \ \& \& (y_i < x_{i-1}) \\ y_i - 1, & \text{if } |y_i - x_{i-1}| > P \ \& \& (y_i > x_{i-1}) \\ y_i, & \text{khác} \end{cases} \quad (20)$$

IV. NÉN ẢNH Y SINH 3D VÀ BẢO MẬT THÔNG TIN CÁ NHÂN

Trong phần này chúng tôi giả sử một hệ thống theo dõi sức khỏe từ xa sử dụng các dữ liệu y sinh khác nhau như ảnh y sinh 3D, tín hiệu điện tim, điện não,... Ảnh y sinh 3D được thu nhận từ các trung tâm y tế rồi truyền lên hệ thống đám mây cùng với một số thông tin nhạy cảm của bệnh nhân. Mô hình gồm hai công đoạn chính: phát và thu. Khối phát thực hiện nén ảnh y sinh đồng thời mã hóa và nhúng thông tin cá nhân, khối thu thực hiện tách thông tin và khôi phục dữ liệu y sinh. Tất cả giai đoạn: nén, mã hóa, nhúng, khôi phục ảnh gốc... được giải thích trong các phần sau.

A. Phía phát



Hình 4. Quá trình nén, mã hóa và nhúng ở phía phát

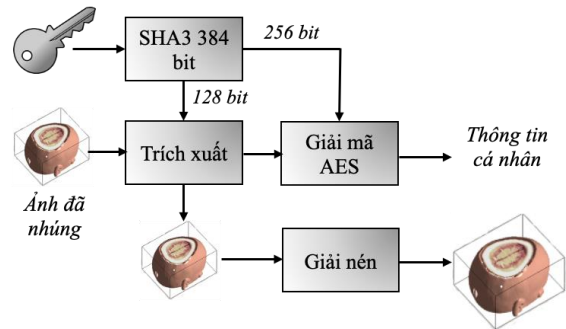
Phía phát sử dụng các ngõ vào để cung cấp cho quá trình truyền tin bao gồm: khóa mật, thông tin cá nhân cần giấu và ảnh y sinh 3D gốc. Hình 4 mô tả các bước thực hiện mã hóa, nén và nhúng thông tin tại phía phát với ngõ ra là ảnh y sinh 3D chứa thông tin mật đã được nén với tỉ lệ phù hợp.

Dữ liệu y sinh 3D gốc ban đầu sẽ được nén bằng kỹ thuật 3D DWT như đã trình bày trong phần II với một tỉ lệ phù hợp. Mục đích của bước này là giảm dung lượng dữ liệu nhưng phải giữ lại được các chi tiết quan trọng của ảnh y sinh 3D. Ngõ ra tại đây sẽ cung cấp cho quá trình nhúng thông tin mà không chấp nhận bất kỳ sự sai khác nào ở đầu thu sau khi ảnh được khôi phục.

Khóa mật ở ngõ vào trước tiên sẽ được tạo chứng thực bởi hàm băm SHA3 [13]. Ngõ ra khỏi này gồm 384 bit sẽ chia làm 2 phần: 256 bit đầu dùng làm khóa cho tầng mã hóa và 128 bit sau dùng làm khóa nhúng. Thông tin cá nhân có thể bao gồm: thông tin nhận dạng, tiền sử bệnh, dị ứng thuốc,... và những thông tin nhạy cảm khác sẽ được mã hóa bởi thuật toán AES [14] với khóa là 256 bit đầu của giá trị băm cung cấp bởi khối SHA3.

Thông tin mật sau khi mã hóa sẽ được nhúng vào ảnh y sinh 3D đã nén với khóa nhúng là 128 bit cuối của giá trị băm. Quá trình nhúng thông tin được thực hiện bằng thuật toán giấu tin thuận nghịch như mô tả trong phần III. Khóa nhúng sẽ được nhúng trước tiên rồi đến kích thước dữ liệu và sau cùng là thông tin đã mã hóa. Như vậy, ngõ ra tại phía phát là dữ liệu y sinh 3D đã được xử lý nén và nhúng thông tin mật. Dữ liệu này sẽ được truyền tới phía thu nhằm bảo mật thông tin cá nhân với độ an toàn cao của các kỹ thuật giấu tin và mã hóa tiên tiến.

B. Phía thu



Hình 5. Quá trình trích xuất, giải mã và giải nén

Phía thu sử dụng dữ liệu y sinh 3D có chứa thông tin mật từ đầu phát gửi đến để kết hợp với khóa mật nhận được từ một kênh an toàn để tiến hành trích xuất thông tin. Các bước thực hiện được mô tả như trong hình 5.

Tương tự như phía phát, khóa mật ở ngõ vào cũng được chứng thực bởi hàm băm SHA3 cho ngõ ra là 384 bit cung cấp cho khối trích xuất và khối giải mã AES. Ảnh y sinh 3D có chứa thông tin mật được đưa qua khối trích xuất thông tin nhằm thực hiện hai nhiệm vụ: bóc tách thông tin cá nhân và khôi phục dữ liệu y sinh 3D gốc. Các bước trích xuất thông tin được mô tả như trong phần III với khóa tách lấy từ 128 bit sau của giá trị băm. Với kỹ thuật giấu tin thuận nghịch đề xuất, thông tin cá nhân và ảnh y sinh 3D sẽ được khôi phục hoàn toàn chính xác. Ảnh y sinh 3D sau khi khôi phục chính xác sẽ cung cấp cho các chuyên gia y tế để tiến hành chẩn đoán bệnh. Thông tin mật sau khi bóc tách được đưa qua khối giải mã

AES với 256bit khóa lấy từ giá trị băm và cho ngõ ra là thông tin cá nhân mà đầu phát muốn gửi đến.

Giả sử tại phía thu, người nhận không có khóa giải mã đúng hoặc có sự sai khác của ảnh đã nhúng so với đầu phát thì tại ngõ ra không tồn tại tin mật và ảnh y sinh 3D cũng không được khôi phục đúng. Trong một số trường hợp, ảnh y sinh 3D cần được khôi phục về độ phân giải gốc nên sẽ được đưa qua khối giải nén cho ngõ ra là ảnh y sinh ban đầu.

V. KẾT QUẢ THỰC NGHIỆM

Các thí nghiệm sau đây được thực hiện trên máy tính core i7, Ram 8 GB với Matlab 2020a. Dữ liệu y sinh 3D mô phỏng với các kích thước khác nhau lấy từ các bộ dữ liệu nổi tiếng như: Viện y tế Quốc gia (NIH) Hoa Kỳ [15], trường đại học Stanford [16], ảnh y khoa DICOM [17] như thể hiện trong bảng I.

Bảng I. Đặc điểm cơ sở dữ liệu mô phỏng

Ảnh 3D	Nguồn	Kích thước	Số lớp
Cthead	[16]	256 x 256	99
Ctscan	[15]	512 x 512	81
Mrbrain	[16]	256 x 256	99
Dicom1	[17]	512 x 512	33
Dicom2	[17]	512 x 512	99

Để đánh giá kết quả mô phỏng, bài báo sử dụng các tham số: sai số bình phương trung bình (MSE – Mean Squared Error) (21) và tỉ lệ tín hiệu đỉnh trên nhiễu (PSNR – Peak Signal to Noise Ratio) (22).

$$MSE = \frac{1}{LMN} \sum_{k=1}^L \sum_{i=1}^M \sum_{j=1}^N (I'_{k,i,j} - I_{k,i,j})^2 \quad (21)$$

Với L, M, N là kích thước khối dữ liệu 3D; $I_{k,i,j}$ và $I'_{k,i,j}$ là giá trị hai khối dữ liệu 3D cần so sánh tại điểm k, i, j .

$$PSNR = 10 \cdot \log_{10} \frac{I_{peak}^2}{MSE} \text{ (dB)} \quad (22)$$

Với I_{peak} là giá trị đỉnh của ảnh I .

Một tham số khác dùng để đánh giá hiệu năng của hệ thống là tỉ lệ nén (CR – Compression Ratio). Đây là tỉ số của số bit ban đầu B_i và số bit sau khi nén B_o . Trong mô hình này, B_i là tổng số bit của dữ liệu mật và ảnh y sinh 3D gốc, trong khi B_o là số bit của ảnh y sinh 3D ở ngõ ra khối phát.

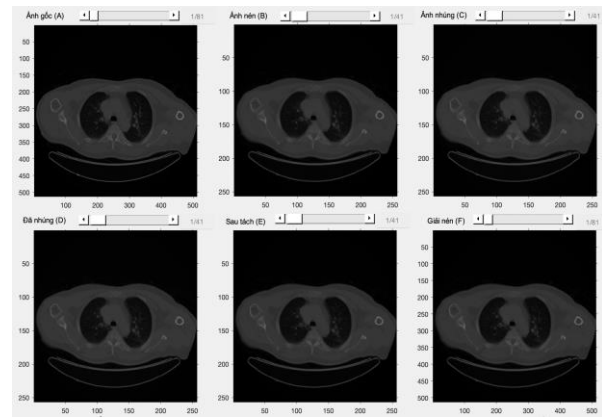
$$CR = \frac{B_i}{B_o} \quad (23)$$

Gọi A, B, C, E, F lần lượt là ảnh y sinh 3D gốc, ảnh đã nén, ảnh sau khi nhúng, ảnh sau khi trích xuất khôi phục và ảnh sau khi giải nén. Hình 6 cho thấy kết quả của toàn bộ quá trình nén, nhúng thông tin mật vào ảnh y sinh 3D Ctscan [16] ở đầu phát và trích xuất thông tin, giải nén ở đầu thu. Hình 7 cho thấy quá trình nén mức 2 và nhúng thông tin mật vào ảnh Dicom2, chúng ta thấy rằng mặc dù đã nén với $CR=63.38$, ảnh ngõ ra vẫn có chất lượng tốt đồng thời thông tin hoàn toàn được bảo mật.

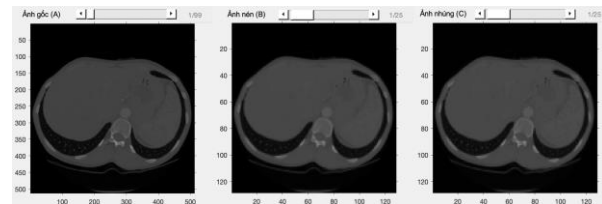
Tại đầu thu, sai số bình phương trung bình $MSE=0$ (so sánh giữa dữ liệu mật nhận được với dữ liệu mật từ đầu

phát gửi đến) trong tất cả các trường hợp cho thấy kết quả bóc tách được là hoàn toàn chính xác đảm bảo tính toàn vẹn dữ liệu. Mặt khác, quá trình bóc tách thông tin cũng đã khôi phục dữ liệu y sinh một cách chính xác, không có bất kỳ một sự sai khác nào của ảnh khôi phục được so với ảnh trước khi nhúng.

Bảng II trình bày kết quả nhúng 1024 byte thông tin cá nhân vào các dữ liệu y sinh khác nhau cùng kỹ thuật nén 3D DWT mức 1. Theo đó chúng ta thấy rằng, thuật toán giấu tin thuận nghịch đã khôi phục hoàn toàn chính xác đối tượng chứa tin qua tham số $PSNR_{B-E} = \infty$ (so sánh giữa ảnh khôi phục và ảnh trước khi nhúng) trong tất cả các trường hợp. Tính vô hình của kỹ thuật nhúng cũng được thể hiện rõ qua tham số $PSNR_{B-C} > 58.4$ dB (so sánh giữa ảnh trước và sau khi nhúng).



Hình 6. Kết quả mô phỏng với tập ảnh Ctscan



Hình 7. Nén và nhúng với CR=63.38 trên tập Dicom2

Bảng II. Kết quả nén và nhúng 1024 byte thông tin

Ảnh 3D	CR	PSNR _{B-C}	PSNR _{B-E}	PSNR _{A-F}
Cthead	7.93	61.83	inf	32.34
Ctscan	7.91	62.37	inf	38.83
Mrbrain	7.93	61.70	inf	35.39
Dicom1	7.77	58.46	inf	41.60
Dicom2	7.92	63.02	inf	42.30

Bảng III. So sánh tính ẩn của dữ liệu sau khi nhúng

Thuật toán	Ảnh chứa	Dữ liệu mật	PSNR _{B-C}
[18]	256 x 256	4096 bit	53.36 dB
Đề xuất	256 x 256	4096 bit	58.72 dB
[19]	512 x 512	2216 bit	45.12 dB
Đề xuất	512 x 512	2216 bit	61.97 dB

Để nhận thấy rõ hơn tính vô hình của thuật toán giấu tin, chúng tôi thực hiện nhúng lần lượt 2216 bit và 4096

bit thông tin vào các ảnh chứa 3D theo đúng tỉ lệ trong [18] và [19], sau đó so sánh ảnh 3D trước và sau khi nhúng ($PSNR_{B-C}$). Kết quả thực nghiệm từ bảng III cho thấy thuật toán đề xuất có tính vô hình cao hơn nhiều so với các nghiên cứu liên quan.

VI. KẾT LUẬN

Bài báo này đã đề xuất một phương pháp bảo mật cho thông tin cá nhân sử dụng các thuật toán mã hóa kết hợp với kỹ thuật giấu tin thuận nghịch trong ảnh y sinh 3D. Ngoài ra để thuận lợi trong quá trình lưu trữ và truyền tin, ảnh y sinh ban đầu cũng đã được nén lại với kỹ thuật nén 3D DWT với nhiều lựa chọn tỉ lệ nén khác nhau. Kết quả thí nghiệm chỉ ra rằng mô hình đề xuất phù hợp với các hệ thống chăm sóc sức khỏe từ xa và thuật toán giấu tin thuận nghịch có tính vô hình cao đồng thời cho kết quả khôi phục dữ liệu hoàn toàn chính xác.

TÀI LIỆU THAM KHẢO

- [1] George C Kagadis 1, Christos Kloukinas, Kevin Moore, Jim Philbin, Panagiotis Papadimitroulas, Christos Alexakos, Paul G Nagy, Dimitris Visvikis, William R Hendee, "Cloud computing in medical imaging". *Med. Phys.* 40(7):070901, 2013. doi:10.1118/1.4811272.
- [2] A. -M. Rahmani et al., "Smart e-Health Gateway: Bringing intelligence to Internet-of-Things based ubiquitous healthcare systems," 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA, 2015, pp. 826-834, doi: 10.1109/CCNC.2015.7158084.
- [3] Teng, C., Mitchell, J., Walker, C., Swan, A., Davila, C., Howard, D., and Needham, T., "A medical image archive solution in the cloud". In: IEEE international conference on software engineering and service sciences (ICSESS), Beijing, China, pp 431-434, 2010 doi: 10.1109/ICSESS.2010.5552343.
- [4] Ayman Ibaida, I. Khalil, R. van Schyndel, "A low complexity high capacity ECG signal watermark for wearable sensor-net health monitoring system", *Computing in Cardiology, IEEE* 2011, pp.393-396.
- [5] V. Sankari, K. Nandhini, "Steganography technique to secure patient confidential information using ECG signal", *IEEE* 2014, Information Communication and Embedded Systems (ICICES), 2014 International Conference on, pp.1-7, 27-28 Feb. 2014.
- [6] B. Halder, S. S. Bose, N. Mishra and S. Mitra, "Embedding and retrieving patient's identification and compression of ECG signal," *Students' Technology Symposium (TechSym)*, 2014 IEEE, Kharagpur, 2014, pp. 1-6.
- [7] D. Ravichandran, M. G. Ahamad and M. R. A. Dhivakar, "Performance analysis of three-dimensional medical image compression based on discrete wavelet transform," 2016 22nd International Conference on Virtual System & Multimedia (VSMM), 2016, pp. 1-8, doi: 10.1109/VSMM.2016.7863176.
- [8] A. Bilgin, G. Zweig, and M. W. Marcellin, "Three-dimensional image compression with integer wavelet transforms," *Applied optics*, vol. 39, pp. 1799-1814, 2000.
- [9] P. L. Dragotti, G. Poggi, and A. R. P. Ragozin, "Compression of Multispectral Images by Three-Dimensional SPIHT Algorithm", *IEEE Transactions on Geoscience and Remote Sensing*, Vol. 38, No. 1, Jan. 2000, pp. 416-428.
- [10] Po-Whei Huang, Yung-Kuan Chan, Chia-Yi Chuang, Hao-Cheng Wang, "Reversible Data Hiding Algorithm Using Dual Domain Embedding", *2nd International Symposium on Computer, Communication, Control and Automation (3CA 2013)*, pp.78-81.
- [11] Celik, Mehmet & Sharma, Gaurav & Tekalp, A. & Saber, Eli. (2005). Lossless generalized-LSB embedding. *IEEE transactions on image processing : a publication of the IEEE Signal Processing Society.* 14. 253-66. 10.1109/TIP.2004.840686.
- [12] C. -C. Chang, W. -L. Tai and K. -N. Chen, "Lossless Data Hiding Based on Histogram Modification for Image Authentication," 2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, Shanghai, China, 2008, pp. 506-511, doi: 10.1109/EUC.2008.20.
- [13] Charles H. Romine, "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions", *Information Technology Laboratory Gaithersburg*, 2014.
- [14] J. Daemen, V. Rijmen, "The Design of Rijndael: AES – The Advanced Encryption Standard", *Springer*, 2002.
- [15] <https://imagej.nih.gov>, truy cập lần cuối vào ngày 18/11/2022.
- [16] <https://graphics.stanford.edu/data/voldata/>, truy cập lần cuối vào ngày 18/11/2022.
- [17] <https://www.dicomlibrary.com/>, truy cập lần cuối vào ngày 18/11/2022.
- [18] Ms. Shubhangi D. Mashalkar, Prof. S. S. Shirgan, "DWT & SVD Based Watermarking Scheme for Copyright Protection In Medical Images", *International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)*, Vol 4, Issue 8, August 2017, ISSN (Online) 2394-232, pp. 125-130.
- [19] Sonika C. Rathi and Vandana S. Inamdar, "Medical images authentication through watermarking preserving ROI", *Health Informatics - An International Journal (HIJ)* Vol.1, No.1, August 2012, pp. 27-42.
- [20] Mostafa A. Ahmad, Mourad Elloumi, Ahmed H. Samak, Ali M. Al-Sharafi, Ali Alqazzaz, Monir Abdullah Kaid, Costas Iliopoulos, "Hiding patients' medical reports using an enhanced wavelet steganography algorithm in DICOM images", *Alexandria Engineering Journal*, volume 61, issue 12, 2022, p. 10577-10592, ISSN 1110-0168.

3D BIOMEDICAL IMAGE COMPRESSION AND PRIVACY PROTECTION

Abstract: This paper proposes a confidential information transmission system combining compression, encryption and hiding algorithms, the aim is to provide a new communication solution to ensure the safety of sensitive and effective personal information. in storage and transmission, while retaining the necessary features of 3D (Three-dimensional) biomedical images. The biomedical image will initially be compressed using 3D wavelet analysis before personal information is embedded using reversible hiding techniques. Personal information and biomedical images before embedding will be completely restored at the receiver, in addition, the AES (Advanced Encryption Standard) encryption algorithm helps to increase the security of personal information.



Nguyễn Lương Nhật, Nhận học vị Tiến sỹ năm 1998 tại Moscow, nước Nga. Hiện là Trưởng khoa Kỹ thuật Điện tử 2, Học viện Công nghệ Bưu chính Viễn thông, cơ sở tại TP. Hồ Chí Minh. Lĩnh vực nghiên cứu: Xử lý tín hiệu, trí tuệ nhân tạo, an toàn thông tin.