KỸ THUẬT GIẤU TIN VÔ HÌNH VÀ BẢO MẬT TRÊN VIDEO 3D

Hoàng Xuân Dương[1,2], Lê Xuân Kỳ[1], Nguyễn Thị Quỳnh Dư[1,2], Nguyễn Thị Minh Thy[1]
[1]Trường Đại học Công Nghệ Sài Gòn
[2]Học viện Kỹ thuật Quân sự

Tóm tắt: *Bài báo trình bày một giải pháp truyền tin mật an toàn sử dụng kỹ thuật giấu tin trong video 3D (3-Dimension) với tính vô hình cao. Thông tin mật được mã hóa bởi các thuật toán mạnh mẽ trước khi nhúng vào video 3D bằng thuật toán LSB (Least Significant Bit) kết hợp. Chỉ những vùng độc lập trên các khung ảnh 3D mới được lựa chọn để nhúng thông tin. Trong khi các thuật toán mã hóa cung cấp độ bảo mật cho thông tin ẩn giấu thì kỹ thuật giấu tin thích nghi sử dụng LSB kết hợp sẽ đảm bảo tính vô hình cao cho thông tin mật.*

Từ khóa: Giấu tin, khớp ảnh, LSB kết hợp, video 3D.

I. GIỚI THIỆU

Ngày nay, kỹ thuật giấu tin trên các dữ liệu đa phương tiện đã trở thành lựa chọn phổ biến để truyền các thông tin nhạy cảm. Tính vô hình là một thước đo chuẩn mực để đánh giá chất lượng của các thuật toán giấu tin. Hệ thống giấu tin được xem là thất bại nếu một kẻ tấn công có thể chứng minh sự tồn tại của thông tin mật bên trong đối tượng chứa, hay được xem là an toàn nếu những kẻ tấn công không thể phát hiện sự hiện diện của các thông điệp ẩn bên trong đối tượng chứa bằng bất kỳ phương pháp tiếp cận nào, vì vậy dữ liệu ẩn phải vô hình cả về mặt nhận thức lẫn thống kê.

Cũng với mục đích bảo mật thông tin, một hướng tiếp cận khác thực hiện mã hóa dữ liệu thành những thông tin vô nghĩa. Sự kết hợp của mật mã và giấu tin sẽ làm tăng độ tin cậy của một kênh thông tin mật, vì ngoài quá trình mã hóa và giải mã, chúng được bổ sung thêm hai quá trình là giấu và tách thông tin. Hệ thống kết hợp này sẽ làm cho các thám mã khó khăn hơn khi phải cố gắng nhận ra đối tượng có ẩn dữ liệu trước khi bóc tách và giải mã chúng. Ngay cả trong các hệ thống sử dụng mật mã yếu hơn cũng rất khó để nhận ra việc truyền tin có ẩn dữ liệu mật bởi tính nguỵ trang cao của các kỹ thuật giấu tin tiên tiến.

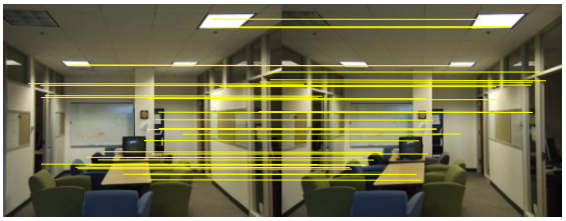
Trong [1], [2] các tác giả đã trình bày phương pháp giấu tin trong miền không gian chủ yếu dùng kỹ thuật LSB. Phương pháp này dễ thực hiện và cũng dễ dàng tấn công và bóc tách thông tin. Trong [3], chúng tôi đã cải tiến thuật toán LSB để tăng tính vô hình cho thông tin mật với sự tham gia của hai pixel liên tiếp theo quy tắc đảo bit, thuật toán đã đạt được mục đích là giảm xác suất thay đổi trên đối tượng chứa về dưới 0.5 trên một bit nhúng.

Nhằm giảm sự nghi ngờ của những kẻ tấn công tìm dữ liệu ẩn, các tác giả trong [4] đề xuất một thuật toán giấu tin thích nghi trên video. Trọng tâm của phương pháp này là việc nhúng dữ liệu trong các vùng da người của các khung ảnh. Trong [5], [6], [7] các tác giả cũng đã thực hiện nhúng thông tin vào vùng đối tượng chuyển động trên video sử dụng thuật toán phát hiện và theo dõi đối tượng chuyển động, video được chọn làm đối tượng chứa là loại 2D thông thường.

Trong [8], chúng tôi đã thực hiện nhúng thông tin mật trên video 3D dùng kỹ thuật parity. Hệ thống này rất an toàn với việc kết hợp các hệ mật mã đối xứng và bất đối xứng, nhưng chưa áp dụng được các phương pháp thích nghi khi chọn lựa các khung ảnh nhúng nên có thể tạo sự nghi ngờ cho các thám mã. Trong nghiên cứu này, các khung ảnh 3D sẽ được xử lý để tìm ra vùng độc lập (không tồn tại trong ảnh còn lại), thông tin mật sau khi mã hóa sẽ được nhúng vào những vùng này. Thuật toán giấu tin LSB kết hợp được phát triển với mục đích giảm xác suất thay đổi trên đối tượng chứa tin về dưới 0.4 đối với một bit nhúng. Hệ thống này là sự kết hợp hoàn hảo giữa các thuật toán mã hóa tiên tiến với kỹ thuật giấu tin thích nghi trên video 3D nhằm cung cấp một hệ thống truyền tin an toàn đồng thời đảm bảo tính vô hình cao cho thông tin mật.

II. SO KHỚP ẢNH STEREO

Ảnh 3D (hay video 3D) ra đời dựa trên nguyên lý tạo ảnh 3 chiều từ hai mắt, sự chìm hay nổi của một vật phụ thuộc vào cách nhìn của người quan sát. Có thể hiểu rằng, mỗi khung ảnh 3D sẽ tồn tại hai ảnh: trái và phải dành cho hai mắt. Hai ảnh này sẽ có độ lệch nhất định giống như khi chúng ta dùng từng mắt để nhìn vào một vật nào đó.



Hình 1. Các cặp điểm đặc trưng SURF tương đồng trong ảnh stereo

Tác giả liên hệ: Hoàng Xuân Dương
Email: duong.hoangxuan@stu.edu.vn
Đến tòa soạn: 8/2018, chỉnh sửa: 10/2018, chấp nhận đăng: 11/2018

Hình 2. Nhận biết vùng độc lập của ảnh stereo dựa trên thuật toán khớp ảnh

Nhận dạng và so khớp ảnh là một trong các hướng nghiên cứu được nhiều nhà khoa học quan tâm trong lĩnh vực thị giác máy tính. Quá trình so khớp ảnh stereo thông thường được chia làm hai giai đoạn chính: xác định các điểm đặc trưng trên các ảnh đơn lẻ, đối sánh và khớp các điểm đặc trưng trên hai ảnh với nhau để tạo thành khối ảnh thống nhất. Từ đó thực hiện các nghiên cứu liên quan như: phân tích độ sâu [9], phát hiện sự khác biệt [10], điều hướng [11]…

Trong giai đoạn đầu, có nhiều thuật toán trích xuất đặc trưng đã được nghiên cứu, trong đó thuật toán SURF (Speeded-Up Robust Features) được sử dụng nhiều nhất bởi ưu điểm về tốc độ cũng như sự bất biến với tỷ lệ và góc xoay [10], [11], [12]. Kết quả của quá trình này là một vector chứa dữ liệu liên quan đến các đặc trưng SURF được phát hiện từ mỗi ảnh.

Giai đoạn thứ hai thực hiện đối sánh các đặc trưng trên hai ảnh dựa vào kết quả phân tích đặc trưng trong giai đoạn đầu. Từng cặp điểm đặc trưng trên hai ảnh sẽ được khớp với nhau dựa vào sự tương quan của chúng. Hình 1 mô tả các cặp điểm đặc trưng SURF tương đồng trong hai ảnh trái, phải và hình 2 chỉ ra những vùng độc lập trên hai ảnh mà chúng không tồn tại trong ảnh còn lại (phần bìa ngoài của ảnh).

III. THUẬT TOÁN GIẤU TIN LSB KẾT HỢP

Trong các nghiên cứu về ẩn dữ liệu, thuật toán LSB được sử dụng phổ biến nhất vì các ưu điểm về tốc độ và dung lượng nhúng. Gắn với tên gọi của nó, thuật toán hoạt động bằng cách lần lượt thay thế các bit ít quan trọng nhất (LSB) của đối tượng chứa bởi các bit thông điệp bí mật. Khi tỉ lệ nhúng là 1 (1 bit / 1 pixel) có thể nhận thấy rằng xác suất để đối tượng chứa bị thay đổi là 0.5 (nhúng 2 bit thì có 1 sự thay đổi).

Xác suất thay đổi trên đối tượng chứa (*Pr*) được định nghĩa là tỉ số của tổng giá trị các thay đổi khi thực hiện nhúng thông tin trên tổng số bit nhúng của tất cả các trường hợp.

$$Pr = \frac{1}{N}\sum_{i=1}^{N}|y_i - x_i| \qquad (1)$$

Với N là số bit nhúng; x, y lần lượt là đối tượng chứa trước và sau khi nhúng.

Nhằm mục đích giảm sự tác động lên đối tượng chứa tin so với kỹ thuật LSB thông thường với cùng dung lượng nhúng, thuật toán LSB kết hợp được phát biểu như sau:

Lần lượt nhúng hai bit dữ liệu mật m_1, m_2 vào 2 pixel x_1, x_2 của ảnh xám tạo thành 2 pixel ngõ ra y_1, y_2 theo (2).

$$y_1, y_2 = \begin{cases} x_1, x_2 & if \quad (x_1 + 2x_2) \bmod 4 = m \\ x_1 + 1, x_2 & if \quad (x_1 + 2x_2) \bmod 4 = m - 1 \\ x_1 - 1, x_2 & if \quad (x_1 + 2x_2) \bmod 4 = m + 1 \\ x_1, x_2 \pm 1 & if \quad (x_1 + 2x_2) \bmod 4 = m \pm 2 \end{cases} \qquad (2)$$

Với $m = 2^1 m_1 + 2^0 m_2 = \{0,1,2,3\} = \{00,01,10,11\}_2$

Lúc này xác suất thay đổi P_r được tính như sau:

$$P_r = P_r(x_1, x_2) + P_r(x_1 + 1, x_2) + P_r(x_1 - 1, x_2) + P_r(x_1, x_2 + 1)$$

$$= \frac{0 \times 1}{8} + \frac{1 \times 1}{8} + \frac{1 \times 1}{8} + \frac{1 \times 1}{8} = \frac{3}{8} = 0.375$$

Tại đầu thu dữ liệu mật được bóc tách theo (3):

$$m' = 2m_1' + m_2' = (y_1 + 2y_2) \bmod 4 \qquad (3)$$

Trường hợp dữ liệu đầu vào có giá trị nằm ở ngưỡng giới hạn cho phép (ví dụ 255 hoặc 0 đối với ảnh 8 bit), nếu áp dụng công thức (2) sẽ xảy ra hiện tượng tràn số học. Khi đó thuật toán được thực hiện như sau:

Giả sử $x_1 = 255$ và ngõ ra cần là $y_1 = x_1 + 1$ ta đổi thành $y_2 = x_2 \pm 1$ và $y_1 = x_1 - 1$. Hoặc $x_1 = 0$ và ngõ ra $y_1 = x_1 - 1$ ta đổi thành $y_2 = x_2 \pm 1$ và $y_1 = x_1 + 1$.

Bảng I sau đây cho thấy sự khác biệt trong quá trình nhúng / tách của thuật toán LSB thay thế và LSB kết hợp với các dữ liệu đầu vào khác nhau.

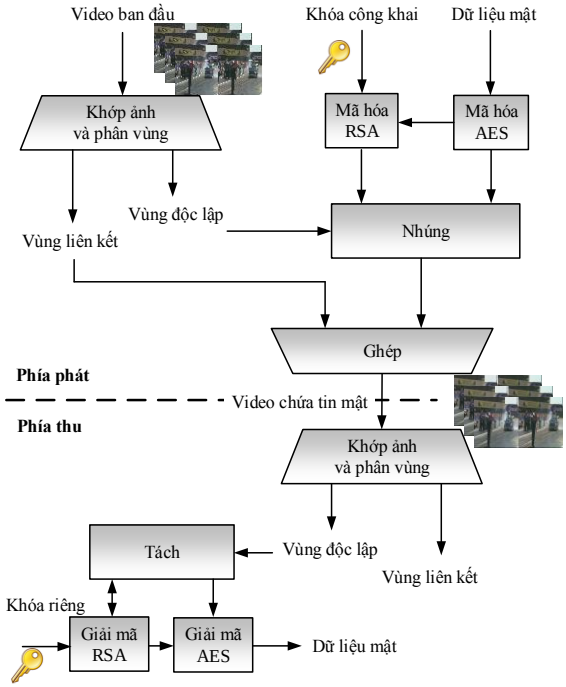
Bảng I. So sánh LSB và LSB kết hợp

Ban đầu		**Dữ liệu mật**	**LSB thay thế**			**LSB kết hợp**			
x_1	x_2	$m=2m_1+m_2$	y_1	y_2	m'	y_1	y_2	y_1+2y_2	m'
5	110	0	**4**	110	0	**4**	110	224	0
5	110	1	**4**	**111**	1	5	110	225	1
5	110	2	5	110	2	**6**	110	226	2
5	110	3	5	**111**	3	5	**109**	223	3
240	165	0	240	**164**	0	240	**164**	568	0
240	165	1	240	165	1	**239**	165	569	1
240	165	2	**241**	**164**	2	240	165	570	2
240	165	3	**241**	165	3	**241**	165	571	3
32	202	0	32	202	0	32	202	436	0
32	202	1	32	**203**	1	**33**	202	437	1
32	202	2	**33**	202	2	32	**201**	434	2
32	202	3	**33**	**203**	3	**31**	202	435	3
Xác suất thay đổi			**12/24 = 0.5**			**9/24 = 0.375**			

IV. MÔ HÌNH ĐỀ XUẤT

Trong phần này chúng tôi đề xuất một giải pháp truyền tin mật sử dụng các thuật toán mã hóa kết hợp với kỹ thuật giấu tin trên video 3D. Để không gây nghi ngờ cho các thám mã, thông tin mật chỉ nhúng vào vùng độc lập trên các khung ảnh 3D. Kỹ thuật giấu tin LSB kết hợp được áp dụng để nhúng thông tin nhằm tăng tính vô hình cho dữ liệu mật. Thuật toán AES (Advanced Encryption Standard) dùng để mã hóa dữ liệu trước khi nhúng để tăng tính bảo mật cho hệ thống. Nhằm giải quyết bài toán trao đổi khóa chúng tôi sử dụng thuật toán RSA (Rivest – Shamir – Adleman) để mã hóa khóa AES và nhúng vào video cùng với dữ liệu đã mã hóa. Mô hình đề xuất được mô tả như hình 3 với chức năng và nguyên lý như sau:

- Khớp ảnh và phân vùng có nhiệm vụ tìm ra các điểm tương đồng giữa hai ảnh trái – phải từ đó đồng nhất hai ảnh này nhằm phân biệt vùng độc lập và vùng liên kết trên khung ảnh.
- *Mã hóa AES* thực hiện mã hóa dữ liệu mật với khóa được tạo ngẫu nhiên trước mỗi lần thực hiện.
- *Mã hóa RSA* thực hiện mã hóa các thông tin định hướng và khóa mật AES.
- Khối *Nhúng* có chức năng giấu các thông tin đã mã hóa vào vùng độc lập của các khung ảnh, sử dụng thuật toán LSB kết hợp.
- Khối *Tách* tại đầu thu thực hiện tách thông tin đã nhúng từ vùng độc lập của các khung ảnh.
- *Giải mã RSA* sử dụng khóa riêng của người nhận để giải mã nhằm tìm ra các thông tin định hướng và khóa mật mà phía phát gửi đến.
- *Giải mã AES* thực hiện giải mã dữ liệu mật từ thông tin tách được và khóa mật lấy được sau khi giải mã RSA.



Hình 3. Mô hình truyền tin mật

Phía phát sử dụng dữ liệu đầu vào gồm: video 3D chứa tin, thông tin mật cần truyền và khóa công khai. Video chứa tin qua các quá trình trích chọn đặc trưng và so khớp ảnh như đã trình bày trong phần II, ngõ ra của quá trình này là các vùng độc lập và vùng liên kết, chỉ những vùng độc lập trong các khung ảnh mới được chọn để nhúng thông tin và chúng được thể hiện qua các mặt nạ ảnh.

Dữ liệu mật trước tiên sẽ được mã hóa bởi thuật toán AES với 256 bit khóa được tạo ngẫu nhiên sau mỗi lần nhúng. Ngoài 256 bit dùng làm khóa mật cho AES, bộ tạo chuỗi giả ngẫu nhiên còn tạo ra các địa chỉ ngẫu nhiên, đây là địa chỉ các khung ảnh dùng để nhúng dữ liệu mật, số lượng khung ảnh phụ thuộc vào kích thước dữ liệu mật cần nhúng và số điểm ảnh trong vùng độc lập của các khung video.

Khóa mật AES, địa chỉ các khung ảnh nhúng cùng với các thông tin khác về kích thước và loại dữ liệu mật sẽ được đóng gói thành một header và mã hóa bởi thuật toán RSA với khóa công khai từ người nhận cung cấp. Trong nghiên cứu này chúng tôi sử dụng khóa RSA có độ dài modulus là 8192 bit. Dữ liệu mật cùng header sau khi mã hóa sẽ được nhúng vào những vùng độc lập trên video theo các mặt nạ lấy từ khối "khớp ảnh và phân vùng", số lượng và thứ tự các khung ảnh được quy định trong header. Sau đó, các khung ảnh sẽ được ghép lại theo đúng thứ tự để tạo thành video 3D đã nhúng dữ liệu mật rồi truyền đến phía thu.

Trong quá trình truyền tin, nội dung ẩn chứa rất khó bị phát hiện vì video là một dạng media phổ biến trên đường truyền và khả năng ngụy trang cao của thuật toán giấu tin đề xuất. Nói cách khác, phương pháp truyền tin này đã làm cho dữ liệu mật gần như vô hình trên đối tượng chứa.

Tương tự như phía phát, video 3D chứa tin ở ngõ vào phía thu sẽ được xử lý chọn ra các vùng ảnh độc lập để tách thông tin. Quá trình tách được chia làm hai giai đoạn: tách header và tách dữ liệu.

Trong giai đoạn đầu, các thông tin về header đã mã hóa được tách ra từ các khung ảnh đầu tiên, quá trình nhúng và tách tin sử dụng thuật toán LSB kết hợp như đã trình bày trong phần III. Header sau khi tách sẽ được giải mã bởi thuật toán RSA với khóa riêng của người nhận, thông tin giải mã được lúc này là: 256 bit khóa AES, thứ tự các khung ảnh chứa tin, dung lượng và định dạng dữ liệu mật. Dựa vào dung lượng và thứ tự các khung ảnh nhúng, quá trình tách thứ hai được thực hiện cho ngõ ra là thông tin mật đã được mã hóa. Thông tin này sau đó được giải mã AES với 256 bit khóa lấy từ header cho ngõ ra là dữ liệu mật từ đầu phát gửi đến. Như vậy dữ liệu mật từ đầu phát đã được truyền an toàn đến phía thu kết thúc một quá trình truyền tin an toàn và bảo mật.

V. KẾT QUẢ THỰC NGHIỆM

Các kết quả sau đây được thực hiện trên Matlab 2016a với dữ liệu mật giả lập bao gồm: 1 logo nhị phân *ieee.tif* có kích thước 120 x 120 pixel, 2 ảnh xám *lena.tif* và *mri.tif* kích thước lần lượt 100 x 100 và 128 x 128 pixel, 1 file text có độ dài 3389 byte và 1 file tín hiệu điện tim 10.000 mẫu (16 bit / mẫu).

Tám đoạn video 3D có cùng độ phân giải 1920 x 1280 với độ dài khác nhau lấy từ cơ sở dữ liệu nhận dạng và xử lý ảnh

của bộ môn Khoa Học Máy Tính, khoa Kỹ Thuật trường Đại học Freiburg, Đức [13] được sử dụng làm đối tượng chứa tin.

Để đánh giá các kết quả mô phỏng chúng tôi sử dụng tham số: MSE (Mean Squared Error) - sai số bình phương trung bình cho bởi (4) và PSNR (Peak Signal to Noise Ratio) - tỉ số tín hiệu đỉnh trên nhiễu cho bởi (5).

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(I'_{i,j} - I_{i,j})^2 \qquad (4)$$

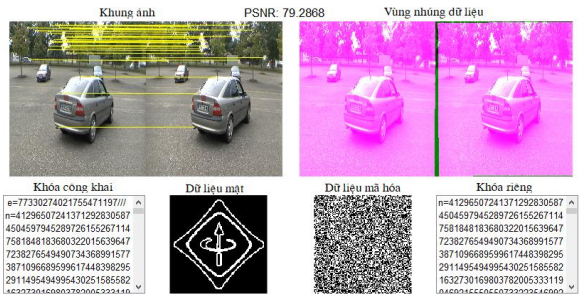
Với: *M, N* là kích thước khối dữ liệu; $I_{i,j}$ và $I'_{i,j}$ là giá trị của các khối dữ liệu tại điểm *i,j*.

$$PSNR = 10.\log_{10}\frac{I_{peak}^2}{MSE}(dB) \qquad (5)$$

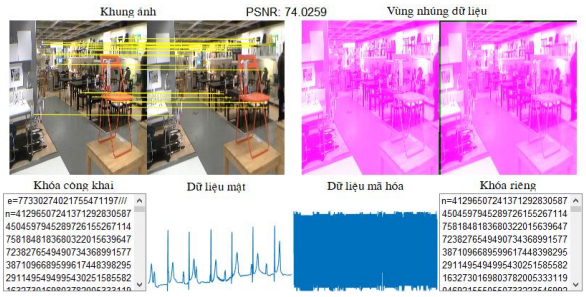
Đối với ảnh 8 bit thì giá trị đỉnh (max) ngõ vào I_{peak} = 255.

Thông thường có thể dùng một trong hai tham số này để đánh giá chất lượng của hệ thống giấu tin, nhưng để dễ dàng so sánh với các nghiên cứu liên quan, trong bài báo này chúng tôi sử dụng cả hai tham số. Trong đó PSNR dùng để so sánh các khung ảnh trước và sau khi nhúng dữ liệu, giá trị này càng cao thì hai ảnh càng giống nhau. MSE dùng để so sánh dữ liệu mật trước khi nhúng và sau khi tách, MSE = 0 khi hai khối dữ liệu hoàn toàn giống nhau.

Hình 4, 5 cho thấy kết quả quá trình phân tích ảnh, mã hóa và nhúng thông tin với dữ liệu giả lập là logo ảnh nhị phân *ieee.tif* và file dữ liệu điện tim *ecg.mat*. Video chứa lần lượt là *car046.m2ts* và *chair013.m2ts* lấy từ tập dữ liệu trong [13]. Kết quả mô phỏng cho thấy mô hình giấu tin đề xuất đã làm dữ liệu mật gần như biến mất trên đối tượng chứa. Ngay cả tham số so sánh PSNR = 74.0259 dB (hình 5) cũng cho thấy tính vô hình cao của thuật toán.



Hình 4. Kết quả nhúng ieee.tif vào video car046.m2ts



Hình 5. Kết quả nhúng ecg.mat vào chair013.m2ts

Tại đầu thu, sai số bình phương trung bình cho thấy dữ liệu bóc tách được là hoàn toàn chính xác (MSE = 0 trong tất cả các trường hợp) đảm bảo tính toàn vẹn dữ liệu. Cần lưu ý rằng tham số MSE thực hiện so sánh dữ liệu mật ban đầu với dữ liệu sau khi bóc tách và giải mã được, trong khi PSNR ở trên so sánh các khung ảnh chứa dữ liệu trong video 3D trước và sau khi nhúng.

Thông tin mật được đảm bảo an toàn bởi các thuật toán mã hóa RSA và AES [14], [15] trong khi tính sẵn sàng vẫn giữ ở mức cao. Bảng II trình bày thời gian trung bình thực hiện các công đoạn mã hóa, giải mã, nhúng và tách thông tin, giá trị này được đo một cách riêng lẻ tại mỗi công đoạn trên các video khác nhau, sau đó lấy trung bình. Theo đó có thể nhận thấy rằng, tổng thời gian thực hiện tại đầu phát (mã hóa – nhúng) và đầu thu (tách – giải mã) đều dưới 1 giây cho thấy tính sẵn sàng cao của hệ thống giấu tin đề xuất.

Để nhận thấy rõ hơn tính vô hình của hệ thống giấu tin đề xuất, chúng tôi thực hiện nhúng lần lượt các dữ liệu mật giả lập vào 8 đoạn video 3D, sau đó so sánh các khung ảnh (có chứa dữ liệu mật) trước và sau khi nhúng sử dụng tham số PSNR. Các kết quả được thể hiện trên bảng III, qua đó chúng ta nhận thấy rằng với PSNR > 73 dB, không thể cảm nhận được sự khác biệt của các khung ảnh sau khi nhúng dữ liệu.

Bảng II. Thời gian (giây) trung bình thực hiện các công đoạn

Công đoạn	Dữ liệu nhúng				
	ieee.tif	***lena.tif***	***mri.tif***	***text.txt***	***ecg.mat***
Mã hóa AES	0.072	0.331	0.528	0.112	0.623
Mã hóa RSA	0.015	0.017	0.014	0.016	0.016
Nhúng	0.095	0.141	0.315	0.132	0.203
Tách	0.098	0.118	0.112	0.051	0.074
Giải mã RSA	0.175	0.168	0.163	0.165	0.162
Giải mã AES	0.126	0.426	0.615	0.143	0.745

Bảng III. Giá trị PSNR (dB) của các khung ảnh trước và sau khi nhúng

Video	Dữ liệu nhúng				
	ieee.tif	***lena.tif***	***mri.tif***	***text.txt***	***ecg.mat***
car046.m2ts	79.2864	73.7351	73.5367	77.4854	72.7371
car049.m2ts	79.2505	75.5059	73.5673	77.5056	74.0115
cat023.m2ts	79.2941	75.4982	74.7997	77.4993	73.9964
cat027.m2ts	79.2791	73.6996	71.7809	77.4866	70.9986
chair013.m2ts	79.2591	75.5423	73.5695	77.5092	74.0188
chair100.m2ts	79.2927	73.7458	73.5746	77.5353	72.7662
dog049.m2ts	79.1860	75.7429	73.5300	77.4686	73.9704

dog050.m2ts	79.2168	75.4735	74.7769	77.4902	74.9518
Trung bình	**79.2581**	**74.8679**	**73.6419**	**77.4975**	**73.4314**

Giả sử rằng thông tin được nhúng vào toàn ảnh (hoặc chỉ nhúng vào vùng liên kết) của các khung ảnh trái - phải trên video 3D, thám mã sẽ dễ dàng phát hiện video chứa thông điệp ẩn dựa vào thuật toán khớp ảnh và trừ nền. Nhưng với kỹ thuật nhúng vào vùng độc lập, phương pháp dò tìm này hoàn toàn không thể phát hiện được thông tin ẩn giấu, vì vậy kỹ thuật giấu tin này sẽ vô hình cả về mặt nhận thức lẫn thống kê.

Vì hệ thống này chỉ nhúng dữ liệu mật vào một phần của các khung ảnh chứa (vùng độc lập) nên tham số PSNR trên bảng III không thể hiện chính xác tính vô hình của thuật toán LSB kết hợp khi so sánh với các nghiên cứu liên quan. Thí nghiệm sau đây thực hiện nhúng 4096 byte dữ liệu mật ngẫu nhiên vào một ảnh chứa có kích thước 512 x 512 pixel với các thuật toán nhúng: LSB kết hợp, LSB thay thế sau đó so sánh kết quả với [3], [8] và [16]. Bảng IV thể hiện hiệu quả nhúng của thuật toán LSB kết hợp khi so sánh với các nghiên cứu liên quan qua tham số PSNR và MSE.

Bảng IV. So sánh hiệu quả nhúng của thuật toán LSB kết hợp với các nghiên cứu liên quan

Thuật toán	Kích thước ảnh chứa	Kích thước dữ liệu mật	PSNR (dB) ảnh chứa	MSE dữ liệu mật
LSB thay thế	512 x 512	4096 byte	64.9221	0
LSB cải tiến [3]	512 x 512	4096 byte	65.7850	0
Parity [8]	512 x 512	4096 byte	64.9185	0
DWT [16]	512 x 512	4096 byte	56.2400	1.042
LSB kết hợp	512 x 512	4096 byte	66.2363	0

VI. KẾT LUẬN

Bài báo này đã đề xuất một phương pháp truyền tin an toàn sử dụng kỹ thuật giấu tin thích nghi trên video 3D kết hợp với các thuật toán mã hóa. Thuật toán giấu tin LSB được phát triển bằng cách kết hợp hai pixel liền kề làm giảm xác suất thay đổi trên đối tượng chứa tin. Thông tin được nhúng vào những thành phần độc lập trên video 3D để không ảnh hưởng đến các liên kết trái – phải của video đồng thời chống lại được các kỹ thuật tấn công và dò tìm tiên tiến. Các kết quả thực nghiệm chứng minh rằng thuật toán đề xuất có tính vô hình rất cao trong khi các tầng mã hóa vẫn đảm bảo an toàn cho thông tin mật.

TÀI LIỆU THAM KHẢO

[1] R. Shreelekshmi, M. Wilscy, C.E. Madhavan, "Cover Image Preprocessing for More Reliable LSB Replacement Steganography", IEEE 2010 International Conference on Signal Acquisition and Processing, pp. 153-156, February 2010.

[2] RigDas, Themrichon Tuithung, "A Novel Steganography Method for Image Based on Huffman Encoding", 2012 IEEE, Emerging Trends and Applications in Computer Science (NCETACS), pp. 14-18.

[3] Nguyễn Lương Nhật, Đào Duy Liêm, Lê Xuân Kỳ, Nguyễn Thị Minh Thy, "Giấu tin thích nghi trên video sử dụng thuật toán theo dõi đối tượng chuyển động và LSB cải tiến", Kỷ yếu Hội thảo quốc gia 2017 về Điện tử, Truyền thông và Công nghệ thông tin, ISBN: 978-604-67-1021-9, pp.116-119.

[4] S. Khupse and N. N. Patil, "An adaptive steganography technique for videos using Steganoflage", in Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014 International Conference on, 2014, pp. 811-815.

[5] Ramadhan J. Mstafa, Khaled M. Elleithy, "A New Video Steganography Algorithm Based on the Multiple Object Tracking and Hamming Codes", 2015 IEEE 14th International Conference on Machine Learning and Applications, pp.335-340.

[6] R. J. Mstafa, K. M. Elleithy and E. Abdelfattah, "A Robust and Secure Video Steganography Method in DWT-DCT Domains Based on Multiple Object Tracking and ECC," in IEEE Access, vol. 5, pp. 5354-5365, 2017, DOI: 10.1109/ACCESS.2017.2691581.

[7] Đào Duy Liêm, Nguyễn Thị Minh Thy, "Chia sẻ thông tin đa truy cập dùng kỹ thuật giấu tin trên video", Kỷ yếu Hội thảo quốc gia lần thứ XIX: Một số vấn đề chọn lọc của Công nghệ thông tin và truyền thông – Hà Nội, 1-2/10/2016, ISBN: 978-604-67-0781-3, pp.67-71.

[8] Nguyễn Lương Nhật, Đào Duy Liêm, Nguyễn Thị Minh Thy, "Giấu tin trong video 3D kết hợp mật mã", Kỷ yếu Hội thảo quốc gia 2014 về Điện tử truyền thông và Công nghệ thông tin – ECIT 2014, pp.366-373.

[9] Dineesh Mohan, Dr. A. Ranjith Ram, "A Review on Depth Estimation for Computer Vision Applications", International Journal of Engineering and Innovative Technology (IJEIT) Volume 4, Issue 11, May 2015, ISSN: 2277-3754, pp. 235-239.

[10] Dennis W. J. M. van de Wouw, Kris van Rens, Hugo van Lint, Egbert G. T. Jaspers, Peter H. N. de With, "Real-time change detection for countering improvised explosive devices", Proc. SPIE 9026, Video Surveillance and Transportation Imaging Applications 2014, 90260T (5 March 2014); DOI: 10.1117/12.2036532.

[11] Eng Zi Hao and Sutthiphong Srigrarom, "Development of 3D Feature Detection and on Board Mapping Algorithm from Video Camera for Navigation", Journal of Applied Science and Engineering, Vol. 19, No. 1, pp. 23-39 (2016) DOI: 10.6180/jase.2016.19.1.04.

[12] Bay, H., A. Ess, T. Tuytelaars, and L. Van Gool. "SURF:Speeded Up Robust Features." Computer Vision and Image Understanding (CVIU).Vol. 110, No. 3, pp. 346–359, 2008.

[13] https://lmb.informatik.uni-freiburg.de/resources/datasets/StereoEgomotion.en.html, truy cập ngày 12/07/2018.

[14] Elaine Barker, Allen Roginsky (2011), "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths", NIST Special Publication 800-131A.

[15] Elaine Barker, William Barker, William Burr, William Polk, Miles Smid (2012), "Recommendation for Key Management – Part 1: General (Revision 3)", NIST Special Publication 800-57.

[16] Aayushi Verma, Rajshree Nolkha, Aishwarya Singh and Garima Jaiswal, "Implementation of Image Steganography Using 2-Level DWT Technique", International Journal of Computer Science and Business Informatics, ISSN: 1694-2108, Vol. 1, No. 1. 2013, pp. 1-14.

[17] Hemalatha S , U Dinesh Acharya , Renuka A , Priya R. Kamath, "A Secure and High Capacity Image Steganography Technique", Signal & Image Processing : An International

Journal (SIPIJ) Vol.4, No.1, February 2013, pp. 83-89, DOI: 10.5121/sipij.2013.4108.

SECURE AND INVISIBLE DATA HIDING TECHNIQUE IN 3D VIDEO

Abstract: This paper presents a solution of transmitting secure and confidential information which is hidden in 3 Dimensional video (3D video) with a high invisibility. The confidential information is encrypted by powerful algorithms before embedding 3D video with the Least Significant Bit (LSB) matching algorithm. Only independent regions on 3D frames are selected for embedding the information. While the cryptographic algorithms provide a security for hidden information, proper cloaking techniques using LSB matching will ensure high invisibility for confidential information.

Hoàng Xuân Dương, Tốt nghiệp Đại học Bách khoa Tp Hồ Chí Minh năm 1997. Hiện là giảng viên khoa Điện Điện tử trường Đại học Công Nghệ Sài Gòn. Lĩnh vực nghiên cứu: Xử lý tín hiệu, mật mã, hệ thống nhúng, công nghệ tri thức.

Lê Xuân Kỳ, Tốt nghiệp Thạc sĩ Kỹ thuật Điện tử năm 2006 tại trường Đại học Bách Khoa Tp Hồ Chí Minh. Hiện là giảng viên khoa Điện Điện tử trường Đại học Công Nghệ Sài Gòn. Lĩnh vực nghiên cứu: Xử lý tín hiệu, đa phương tiện, khai phá dữ liệu, học máy.

Nguyễn Thị Quỳnh Dư, Tốt nghiệp Đại học ngành Điện tử Viễn thông tại Học viện Công nghệ Bưu chính Viễn thông. Hiện là giảng viên khoa Điện Điện tử trường Đại học Công Nghệ Sài Gòn. Lĩnh vực nghiên cứu: Xử lý ảnh, khai phá dữ liệu, học máy.

Nguyễn Thị Minh Thy, Tốt nghiệp Thạc sĩ Kỹ thuật Điện tử năm 2011 tại Học viện Công nghệ Bưu chính Viễn thông. Hiện là giảng viên khoa Điện Điện tử trường Đại học Công Nghệ Sài Gòn. Lĩnh vực nghiên cứu: Xử lý tín hiệu, mật mã, quang vô tuyến, công nghệ tri thức.