PHƯƠNG PHÁP CHỌN ĐIỂM TẤN CÔNG CHO TẤN CÔNG MẪU DỰA TRÊN PHÂN BỐ CHUẨN

Trần Ngọc Quý*, Hoàng Văn Quân*
*Học viện Kỹ thuật Mật mã

Tóm tắt: *Tấn công mẫu được xem như là tấn công kênh kề hiệu quả nhất. Để tấn công mẫu có thể thực hiện được trong thực tế, ta phải lựa chọn một số điểm tấn công trên vết điện năng tiêu thụ thực tế của thiết bị. Cho tới nay có nhiều phương pháp để lựa chọn các điểm này cho tấn công mẫu. Tuy nhiên, các cách lực chọn này dựa trên kinh nghiệm về tấn công kênh kề, đồng thời chưa có công trình nào chỉ ra rằng các phương pháp lựa chọn đó đã là tốt nhất hay chưa. Trong bài báo này, chúng tôi đưa ra một phương pháp lựa chọn điểm mới theo nguyên tắc, khác với các phương pháp đã được thực hiện, dựa trên các các điểm có phân bố xấp xỉ phân bố chuẩn. Việc kiểm chứng kết quả, thấy rằng hiệu năng tấn công mẫu được cải thiện rõ rệt so với các phương pháp tấn công mẫu hiện tại. Thí nghiệm tấn công mẫu trong bài báo được thực hiện trên thẻ thông minh ATMEGA8515 được cài đặt thực thi thuật toán mật mã AES-128.*

Từ khóa: Tấn công kênh kề, tấn công mẫu, phân bố chuẩn, kiểm định Chi bình phoɪơng.

I. MỞ ĐẦU

Tấn công kênh kề là một trong những lỗ hổng nguy hiểm nhất hiện nay khi cài các thuật toán mật mã trên thiết bị. Ý tơởng cơ bản của nó là việc xác định khóa của thiết bị mật mã dựa trên việc phân tích điện năng tiêu thụ [1,2], bức xạ điện từ trơờng [3], thời gian thực hiện lệnh của thiết bị. Các thuật toán mật mã thơờng đơợc chứng minh sự đảm bảo an toàn về mặt toán học mà chơa quan tâm đến việc an toàn cài đặt để chống lại các dạng tấn công kênh kề và rất nhiều hệ mật đã bị tấn công bởi các tấn công này.

Tấn công phân tích điện năng tiêu thụ nhận đơợc sự quan tâm lớn trong các dạng tấn công kênh kề bởi hiệu quả và khả năng thực hiện khá dễ dàng trong điều kiện phòng thí nghiệm. Do đó, bài báo này tập trung vào phân tích tấn công mẫu, một phoɪơng pháp hiệu quả nhất trong tấn công phân tích điện năng tiêu thụ trên khía cạnh lý thuyết thông tin. Đơợc đề xuất bởi Chari [4], năm 2002, tấn công mẫu dựa trên giả định rằng ta có một thiết bị mẫu giống với thiết bị cần tấn công và có thể có toàn quyền truy nhập vào nó. Chính bởi vậy, ta có thể xây dựng chính xác về đặc tính tiêu thụ điện năng của thiết bị cần tấn công. Và tấn công này là một công cụ hữu hiệu để đánh giá độ an toàn vật lý của thiết bị mật mã [4].

Tấn công mẫu đơợc thực hiện qua hai pha: pha lập mẫu, và pha tấn công. Trong pha lập mẫu, ta xây dựng bộ mẫu của mỗi hoạt động có phụ thuộc vào khóa của thiết bị mẫu từ các vết điện năng tiêu thụ, từ nay gọi là trace [5], thu thập đơợc trong quá trình thiết bị hoạt động. Ở pha tấn công, ta thu thập một số nhỏ các trace từ thiết bị cần tấn công và bộ mẫu đã có để tìm ra khóa đúng nhất của thiết bị.

Các trace thơờng chứa nhiều mẫu do tốc độ lấy mẫu của lớn của thiết bị đo, bởi vậy không phải tất cả các mẫu trên trace sử dụng để xây dựng tập mẫu. Để giảm số lơợng mẫu và xây dựng bộ mẫu nhỏ gọn, chỉ một số mẫu quan trọng trên trace đơợc giữ lại, các mẫu này gọi là các POI. Các phơơng pháp lựa chọn POI cho tấn công mẫu hiện tại chọn các điểm chứa nhiều thông tin nhất về những hoạt động có phụ thuộc vào khóa của thiết bị. Tấn công mẫu trong [4], sử dụng cách tiếp cận này để tìm POI. Hơn nữa, các bài báo [6] [7] [8] [9] đề xuất các phoɪơng pháp lựa chọn POI dựa trên cách tiếp cận này. Trong đó, ta chỉ chọn một điểm trong một chu kỳ đồng hồ làm POI do các điểm khác ở cùng chu kỳ đồng hồ không chứa thông tin. Các phơơng pháp dựa trên cách tiếp cận này có thể kể ra nhoɪ chọn POI dựa trên phân tích toɪơng quan (CPA) của các trace [10], tổng bình phoɪơng từng cặp của độ lệch các giá trị trung bình – SOST dựa trên kiểm định T-test [9], độ lệch của các giá trị trung bình - DoM, tổng độ lệch bình phơơng-SOSD (sum of differient of means squared), độ lớn của giá trị tín hiệu trên nhiễu - SNR [10]. Khi lựa chọn các phoɪơng pháp trên để chọn POI ta phải ơớc lơợng độ lớn tín hiệu tại mỗi điểm P_{t_i}. Ví dụ nhoɪ khi sử dụng CPA, SSE(t) đơợc xác định bởi hệ số toơng quan giữa điện năng tiêu thụ thực tế với điện năng tiêu thụ giả thiết tại điểm P_t. Với cách tiếp cận trên, trong một chu kỳ clock, chỉ có một điểm với giá trị SSE lớn nhất đơợc lựa chọn.

Tuy nhiên, cho tới nay, vẫn chơa biết các phơơng pháp lựa chọn POI ở trên đã là tối ơu nhất hay chơa, và có phải là phoɪơng pháp lựa chọn giúp ta quyết định khóa đúng tốt nhất ở pha tấn công không. Do đó, trong bài báo này, chúng tôi tập trung làm sáng tỏ vấn đề này. Trơớc hết bài báo trình bày cách tiếp cận mới cho tấn công mẫu với nguyên tắc khác hoàn toàn so với các phơơng pháp trên. Sự đúng đắn về mặt lý thuyết sẽ đơợc chứng minh nhờ áp dụng tính chất toán học của phân bố Gauss chuẩn đa biến và phơơng pháp kiểm định độ khớp mẫu Chi bình phoɪơng của Pearson. Tiếp đến, chúng tôi trình bày phần thực nghiệm và chỉ ra rằng hiệu quả việc phân lớp tăng lên đáng kể.

Bài báo này đơợc tổ chức nhoɪ sau. Một số cơ sở toán học đơợc sử dụng trong bài báo trình bày ở phần 2. Phần 3 giới thiệu tổng quan về tấn công mẫu. Tấn công mẫu sử dụng phoɪơng pháp lựa chọn POI dựa trên phân bố chuẩn đơợc trình

Tác giả liên hệ: Trần Ngọc Quý
Email:quyhvm@gmail.com
Đến tòa soạn: 10/2018, chỉnh sửa: 12/2018, chấp nhận đăng: 12/2018.

bày ở phần 4. Và phần 5, thực nghiệm tấn công mẫu và các kết quả được trình bày.

II. MỘT SỐ CƠ SỞ TOÁN HỌC

Trong phần này, bài báo giới thiệu một số khái niệm toán học được sử dụng như hàm *Gamma* và phân bố *Chi* bình phương. Tiếp đến khái niệm để kiểm tra độ khớp của mô hình thống kê và phương pháp kiểm tra độ khớp dựa trên phân bố *Chi* bình phương của Pearson được trình bày.

Định nghĩa 1. Hàm *Gamma* được định nghĩa như sau:

$$\Gamma(x) = \int_0^{\infty} e^{-t}t^{x-1}dt\,; với\ x > 0 \qquad (1)$$

Định nghĩa 2. Hàm mật độ xác suất của phân bố *Chi* bình phương với k bậc tự do (ký hiệu: χ_k^2) là:

$$f(x;k) = \begin{cases} \dfrac{1}{\Gamma\left(\frac{k}{2}\right).e^{\frac{k}{2}}} e^{\left(-\frac{x}{2}\right)} e^{\frac{k-2}{2}}, & x > 0 \\ 0, & x \le 0 \end{cases} \qquad (2)$$

Trong đó $\Gamma(.)$ là ký hiệu hàm *Gamma*.

Độ khớp của một mô hình thống kê mô tả mô hình này khớp với một tập mẫu quan sát được như thế nào. Đo độ khớp thường tổng hợp sự khác nhau giữa các giá trị quan sát được và các giá trị kỳ vọng của một mô hình thống kê. Việc đo độ khớp có thể được sử dụng trong kiểm định giả thiết thống kê. Kiểm định *Chi* bình phương của Pearson được sử dụng để kiểm tra sự khác nhau của phân bố tần suất của các mẫu quan sát so với phân bố lý thuyết. Phần tiếp theo, chúng tôi sơ lược về kiểm định *Chi* bình phương.

Giả sử rằng, có một tập hợp X tuân theo một phân bố lý thuyết như sau:

$$H_0: \Pr[X = a_i] = f_i \quad với\ i = 1,2,\dots k$$

Trong đó, $a_i, f_i\ (i = 1,2,\dots,k)$ đã biết và $a_1, a_2, \dots, a_k$ khác nhau từng đôi một, $f_i > 0\ (i = 1,2,\dots,k)$.

Giả sử ta có n mẫu $(X_1, X_2, \dots, X_n)$ từ một biến ngẫu nhiên X và sử dụng kiểm định *Chi* bình phương kiểm tra giả thiết H_0 có đúng hay không. Chúng ta sử dụng ký hiệu ω_i cho số lượng mẫu trong $X_1, X_2, \dots, X_n$ có giá trị là a_i. Nếu giá trị n đủ lớn, ta sẽ có $\frac{\omega_i}{n} \approx f_i$, hay $\omega_i \approx nf_i$. Giá trị nf_i có thể xem như giá trị lý thuyết (ký hiệu TV) cho nhóm a_i. Giá trị ω_i có thể xem như giá trị quan sát được, hay giá trị thực tế (ký hiệu EV) của nhóm a_i. Bảng 1 chỉ ra một số giá trị TV và EV của nhóm a_i.

Bảng 1. Giá trị TV và EV của mỗi nhóm

Nhóm	a_1	a_2	...	a_i	...	a_k
TV	nf_1	nf_2	...	nf_i	...	nf_k
EV	ω_1	ω_2	...	ω_i	...	ω_k

Rõ ràng nếu độ khác biệt hai hàng ở Bảng 1 càng nhỏ thì giả thiết về H_0 có độ đúng càng tăng. Kiểm định *Chi* bình phương của Pearson là phương pháp được biết đến rộng rãi để đo độ khác biệt bởi công thức sau:

$$Z = \sum_{i=1}^{k} \frac{(nf_i - \omega_i)^2}{nf_i} \qquad (3)$$

Z được sử dụng để kiểm tra giả thiết H_0 có đúng hay không. Ví dụ, khi ta lựa chọn một hằng số Con dưới một mức cho trước, khi $Z \le Con$, ta sẽ chấp nhận giả thiết H_0. Còn nếu $Z > Con$ ta sẽ từ chối giả thiết H_0. Bây giờ ta sẽ xem xét trường hợp tổng quát bằng sử dụng bổ đề của Pearson về Z [11].

Bổ đề 1. *Nếu giả thiết H_0 đúng, khi $n \to \infty$, phân bố của Z sẽ xấp xỉ phân bố Chi bình phương với $k-1$ bậc tự do, ký hiệu là χ_{k-1}^2.*

Giả sử rằng ta tính được giá trị cụ thể của Z là Z_0 của một nhóm cụ thể. Đặt:

$$L(Z_0) = \Pr(Z \ge Z_0 | H_0) \approx 1 - K_{n-1}(Z_0) \qquad (4)$$

Trong đó, ký hiệu $K_{k-1}(.)$ là hàm phân bố của χ_{k-1}^2. Rõ ràng khi xác suất $L(Z_0)$ càng lớn, giả thiết H_0 càng đúng. Do đó, xác suất $L(Z_0)$ có thể được sử dụng là công cụ để kiểm định giả thiết H_0.

Nếu phân bố theo lý thuyết của X là liên tục, kiểm định về độ phù hợp *Chi* bình phương của Pearson vẫn đúng. Trong trường hợp này, giả sử ta muốn kiểm định giả thiết:

$$H_1: hàm\ phân\ bố\ của\ biến\ X\ là\ F(x).$$

Hàm phân bố $F(x)$ là liên tục. Để kiểm định giả thiết H_1, ta có thể đặt:

$$-\infty = a_0 < a_1 < a_2 < \cdots < a_{k-1} < a_k = +\infty$$

Và:

$$I_1 = (a_0, a_1], \dots, I_i = (a_{i-1}, a_i], \dots, I_k = (a_{k-1}, a_k).$$

Khi ta có n mẫu $(X_1, X_2, \dots, X_n)$ từ biến ngẫu nhiên X. Gọi ω_i là số phần tử của tập hợp $\{X_j | X_j \in I_i, j \in \{1,2,\dots,n\}\}$ và

$$f_i = \Pr(x \in I_i, x \leftarrow X) = F(a_i) - F(a_{i-1})$$
$$với\ (i = 1,2,\dots,k)$$

Tương tự, sau đó, ta có thể tính $L(Z_0)$ từ phương trình (4) để kiểm định giả thiết H_1.

III. NGUYÊN LÝ TẤN CÔNG MẪU

Tấn công mẫu cơ bản được thực hiện qua hai pha: pha lập mẫu và pha tấn công. Trong pha lập mẫu, chúng ta sử dụng giá trị trung bình và ma trận hiệp phương sai của để mô hình rò rỉ điện năng tiêu thụ của thiết bị. Trong pha tấn công, ta sử dụng nguyên tắc khả năng đúng lớn nhất để tìm khóa đúng của thiết bị tấn công.

A. Pha lập mẫu

Để thực thi tấn công mẫu chúng ta cần một cặp thiết bị giống nhau được gọi tương ứng là thiết bị mẫu và thiết bị để tấn công. Với tấn công mẫu, chúng ta mong muốn tìm được thông tin về khóa $k^s \in \mathbb{K}$ được xử lý bởi thiết bị tấn công tại

một thời điểm nào đó. Với bộ vi điều khiển 8 bít, $\mathbb{K} = \{0,1,\dots,255\}$ là tập các giá trị có thể có của k^s đợc xử lý bởi một lệnh của vi điều khiển.

Chúng ta giả sử rằng có thể biết đợc thời điểm giá trị bí mật k^s đợc xử lý bởi thiết bị để tấn công và đo đợc các vết điện năng tiêu thụ, còn gọi là trace, của thiết bị khi nó xử lý với giá trị bí mật này. Có thể coi các trace là các vector rò rỉ của thiết bị, x^d, mỗi vector có độ dài m^d, ứng với m^d giá trị điện năng tiêu thụ tại các thời điểm $\{t_1, t_2, \dots, t_{m^d}\}$. Nhợ vậy, ta có $x^d \in \mathbb{R}^{m^d}$ vector mô tả trace của thiết bị tấn công tại các thời điểm quanh thời điểm nó xử lý giá trị k^s.

Trong quá trình xây dựng bộ mẫu từ thiết bị mẫu, chúng ta đo n_p vector rò rỉ $x_{ki}^d \in \mathbb{R}^{m^d}$ tợng ứng với mỗi giá trị $k \in \mathbb{K}$, đợc thiết bị xử lý với một hoặc nhiều lệnh, kết hợp chúng thành ma trận rò rỉ $X_k^d \in \mathbb{R}^{n_p \times m^d}$.

Thợng thì, các vector rò rỉ x_{ki}^d chứa một số lợng mẫu m^d lớn do tốc độ lấy mẫu lớn của các thiết bị đo. Do đó, ta thợng phải nén hay làm giảm số lợng mẫu này trợc khi đợa vào xử lý bằng cách chỉ lựa chọn $m \ll m^d$ mẫu. Nhợ vậy, sau khi nén ta có các vector rò rỉ là $x_{ki} \in \mathbb{R}^m$, kết hợp thành ma trận $X_k \in \mathbb{R}^{n_p \times m}$.

Bây giờ, ta sử dụng X_k để tính các tham số cho mẫu tợng ứng với thiết bị xử lý giá trị $k \in \mathbb{K}$ đó là $\bar{x}_k \in \mathbb{R}^m$ và $S_k \in \mathbb{R}^{m \times m}$ nhợ sau:

$$\bar{\boldsymbol{x}}_k = \frac{1}{n_p}\sum_{l=0}^{n_p} \boldsymbol{x}_{ki} \qquad (5)$$

$$\boldsymbol{S}_k = \frac{1}{n_p - 1}\sum_{i=1}^{n_p} (x_{ki} - \bar{\boldsymbol{x}}_k)(x_{ki} - \bar{\boldsymbol{x}}_k)' \qquad (6)$$

Giá trị mẫu của các vết điện năng tiêu thụ có thể xấp xỉ theo phân bố chuẩn đa biến [15]. Nhợ vậy, các giá trị trung bình mẫu $\bar{x}_k$ và $\boldsymbol{S}_k$ là đủ để mô tả thống kê cho giá trị điện năng tiêu thụ của thiết bị theo hàm mật độ xác suất (3).

$$f(x|\,\bar{\boldsymbol{x}}_k, \boldsymbol{S}_k) = \frac{1}{\sqrt{(2\pi)^m \det(\boldsymbol{S}_k)}} \exp\left(-\frac{1}{2}(\boldsymbol{x} - \bar{\boldsymbol{x}}_k)'\boldsymbol{S}_k^{-1}(\boldsymbol{x} - \bar{\boldsymbol{x}}_k)\right) \qquad (7)$$

Nói tóm lại, trong pha lập mẫu, ta sẽ lập $|\mathbb{K}|$ bộ mẫu, mỗi bộ mẫu tợng ứng với một giá trị trung bình và ma trận hiệp sai: $\bar{\boldsymbol{x}}_k, \boldsymbol{S}_k$ tợng ứng với $|\mathbb{K}|$ giá trị bí mật của thiết bị.

B. Pha tấn công

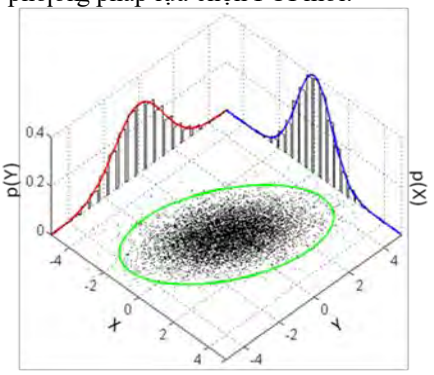
Trong pha tấn công, chúng ta tìm giá trị bí mật $k^s \in \mathbb{K}$ đợc xử lý bởi thiết bị để tấn công. Chúng ta thu thập n_a vector rò rỉ $\boldsymbol{x}_i \in \mathbb{R}^m$ từ thiết bị để tấn công, sử dụng cùng kỹ thuật thu thập và phợng pháp nén với pha lập mẫu. Nhợ vậy ta sẽ có ma trận rò rỉ $\boldsymbol{X}_{ks} \in \mathbb{R}^{n_a \times m}$. Để xác định giá trị bí mật k^s đợc xử lý bởi thiết bị khi biết đợc một vector rò rỉ $\boldsymbol{x}_i \in \boldsymbol{X}_{ks}$, chúng ta có thể áp dụng công thức Bayes. Điều này dẫn tới luật quyết định nhợ sau [8,9,7,6].

$$k^s = \underset{k \in \mathbb{K}}{\operatorname{argmax}}\, P(k|x_i) = \underset{k \in \mathbb{K}}{\operatorname{argmax}}\, P(x_i|k).P(k) \qquad (8)$$

Trong đó, $P(x_i|k) = f(x_i|\bar{x}_k, S_k)$, đợc tính bởi (7), và $P(k^s)$ là xác suất tiên nghiệm của giá trị bí mật k^s. Luật quyết định này cho ta biết vector rò rỉ x_i thuộc một trong các bộ mẫu có giá trị k^s với xác suất hậu nghiệm lớn nhất. Trong trợng hợp tổng quát, ta có $P(k) = |\mathbb{K}|^{-1}$. Luật quyết định khóa đúng trong trợng hợp này dựa trên nguyên tắc khả năng đúng lớn nhất.

IV. PHƯƠNG PHÁP LỰA CHỌN MẪU DỰA TRÊN PHÂN BỐ CHUẨN

Trong phần này, bài báo trình bày phợng pháp tiếp cận mới trong việc lựa chọn POI cho tấn công mẫu. Trợc hết chúng tôi đợa ra bổ đề 2 và đợc chứng minh để làm cơ sở cho phợng pháp lựa chọn POI mới.



Hình 1. Ví dụ về phân bố biên của phân bố Gauss đa biến

Bổ đề 2. *Phân bố của biến đơn trong phân bố Gauss đa biến có phân bố chuẩn*

Hình 1 mô tả phân bố của biến đơn trong phân bố chuẩn đa biến ở đợng màu đỏ và xanh da trời. Các điểm nằm trong đợng elip xanh lá cây tợng ứng với các điểm của phân bố chuẩn hai biến X và Y.

Chứng minh:

Để đơn giản ta chứng minh với trợng hợp phân bố chuẩn 2 biến, $N = 2$. Với các trợng hợp khác, tợng tự, bổ đề này vẫn đúng.

Gọi (ξ, η) là một vector ngẫu nhiên hai chiều. Hàm xác suất tích lũy và hàm mật độ xác suất của vector trên lần lợt là $F(x,y)$ và $f(x,y)$. Các hàm phân bố xác suất của các biến đơn đợc xác định nhợ sau:

$$F_1(x) = \int_{-\infty}^{x}\int_{-\infty}^{\infty} f(u,y)\,du\,dy\,;$$
$$F_2(y) = \int_{-\infty}^{\infty}\int_{-\infty}^{y} f(u,x)\,dx\,du$$

Hàm mật độ xác suất biên đợc xác định nhợ sau:

$$f_1(x) = \int_{-\infty}^{\infty} f(x,y)\,dy\,;\; f_2(y) = \int_{-\infty}^{\infty} f(x,y)\,dx$$

Với phân bố Gauss đa biến hai chiều, ta có hàm mật độ xác suất như sau:

$$f(x,y) = \frac{1}{2\pi|S|}\exp(-\frac{1}{2}(x-a, y-b).S^{-1}.(x-a, y-b)')$$

Trong đó: $S = \begin{pmatrix} \sigma_1^2 & r\sigma_1\sigma_2 \\ r\sigma_1\sigma_2 & \sigma_2^2 \end{pmatrix}$

Và các giá trị $a, b, \sigma_1, \sigma_2, r$ không đổi, $\sigma_1 > 0, \sigma_2 > 0, |r| < 1$. Hàm mật độ xác suất $f(x,y)$ có thể viết như sau:

$$f(x,y) = \frac{1}{2\pi\sigma_1\sigma_2\sqrt{1-r^2}}\exp\left(\frac{-1}{2(1-r^2)}\left[\frac{(x-a)^2}{\sigma_1^2} - \frac{(2r(x-a)(y-b))}{(\sigma_1\sigma_2)} + \frac{(y-b)^2}{\sigma_2^2}\right]\right).$$

Đặt:

$$\frac{x-a}{\sigma_1} = u; \frac{y-b}{\sigma_2} = v$$

Và ta có:

$$f_1(x) = \int_{-\infty}^{\infty} f(x,y)dy$$

$$= \frac{1}{2\pi\sigma_1\sqrt{1-r^2}}\int_{-\infty}^{\infty}\exp\left(-\frac{1}{2(1-r^2)}.(u^2 - 2ruv + v^2)\right)dv$$

$$= \frac{1}{\sqrt{(2\pi)}\sigma_1}e^{-\frac{u^2}{2}}\int_{-\infty}^{\infty}\left(\frac{1}{\sqrt{2\pi(1-r^2)}}\exp\left(-\frac{r^2u^2 - 2ruv + v^2}{2(1-r^2)}\right)\right)dv$$

$$= \frac{1}{\sqrt{2\pi}\sigma_1}e^{-\frac{u^2}{2}}\int_{-\infty}^{\infty}\frac{1}{\sqrt{2\pi(1-r^2)}}\exp\left(-\frac{(v-ru)^2}{2(1-r^2)}\right)dv$$

$$= \frac{1}{\sqrt{2\pi}\sigma_1}e^{-\frac{u^2}{2}} = \frac{1}{\sqrt{2\pi}\sigma_1}\exp(-\frac{(x-a)^2}{2\sigma_1^2})$$

Do đó, $f_1(x)$ có hàm mật độ xác suất của phân bố chuẩn $\mathcal{N}(a, \sigma_1^2)$. Tương tự, ta cũng có:

$$f_2(x) = \frac{1}{\sqrt{2\pi}\sigma_2}\exp(-\frac{(x-b)^2}{2\sigma_2^2})$$

Như vậy, bổ đề 2 được chứng minh.

Ý tưởng chính trong cách tiếp cận để lựa chọn POI như sau. Trong tấn công mẫu, sự phân bố nhiễu tại các điểm POI có phân bố Gauss đa biến [10]. Hơn nữa, dựa vào bổ đề 2, chúng ta biết rằng phân bố của các điểm riêng lẻ của phân bố Gauss đa biến cũng tuân theo phân bố chuẩn. Do đó, trong tấn công mẫu, nếu sự phân bố của các mẫu tại các điểm POI được tuân theo phân bố chuẩn thì mô hình xác suất phân bố Gauss đa biến sẽ tăng độ phù hợp khi sử dụng để xây dựng các bộ mẫu cho tấn công. Nếu không, khi sự phân bố của các mẫu POI không tuân theo phân bố chuẩn thì việc lập mẫu xấp xỉ theo phân bố Gauss đa biến là không tốt dẫn tới hiệu quả tấn công mẫu sẽ không cao. Do đó, cách tiếp cận của bài báo là lựa chọn các mẫu mà sự phân bố các mẫu của nó xấp xỉ phân bố chuẩn hơn các mẫu khác trong một chu kỳ clock như là các điểm POI. Phương pháp lựa chọn POI được đề xuất được gọi là NDB-POI.

Phương pháp kiểm định *Chi* bình phương được sử dụng để kiểm tra độ khớp được sử dụng để kiểm tra sự phân bố của các mẫu tại mỗi điểm có xấp xỉ được phân bố chuẩn hay không. Cụ thể là, giả sử tại một điểm P_t chúng ta có n mẫu $(X_1, X_2, \dots, X_n)$ cho một phép toán cố định với dữ liệu cố định và tính:

$$\hat{\mu} = \frac{1}{n}.\sum_{i=1}^{n} X_i \; ; \; s^2 = \frac{1}{n-1}.\sum_{i=1}^{n}(X_i - \hat{\mu})^2 \qquad (9)$$

Chú ý rằng, trong tấn công mẫu, ta có thể cho thiết bị mẫu thực hiện lệnh bao nhiêu lần cũng được và lấy mẫu một số lượng lớn các trace trong pha lập mẫu. Do đó giá trị của n có thể lấy đủ lớn. Khi n đủ lớn, ta có thể giả sử phân bố lý thuyết của các mẫu tại điểm P_t tuân theo phân bố chuẩn $\mathcal{N}(\hat{\mu}, s^2)$ và để kiểm tra nó có đúng không ta sử dụng kiểm định *Chi* bình phương của Pearson. Hàm phân bố xác suất của phân bố chuẩn được ký hiệu là $F(x; \hat{\mu}, s^2)$.

Đặt:

$$a_0 = -\infty, a_1 = \hat{\mu} - 2s, a_2 = \hat{\mu} - 1.5s,$$
$$\dots, a_9 = \hat{\mu} + 2s, a_{10} = +\infty$$
$$I_1 = (-\infty, \hat{\mu} - 2s], I_2 = (\hat{\mu} - 2s, \hat{\mu} - 1.5s),$$
$$\dots., I_{10} = (\hat{\mu} + 2s, +\infty)$$

Sau đó ta tính:

$$Z_0 = \sum_{i=1}^{10}\frac{(nf_i - \omega_i)^2}{nf_i} \qquad (10)$$

$$với: \; f_i = F(a_i; \hat{\mu}, s^2) - F(a_{i-1}; \hat{\mu}, s^2)$$
$$và \; \omega_i = |\{X_j | X_j \in I_i, j \in \{1,2,\dots,n\}\}|$$

Sau khi có Z_0 ta tính giá trị $L(Z_0)$ sử dụng phương trình (2). Khi giá trị n đủ lớn, nếu các mẫu $\{X_1, X_2, \dots, X_n\}$ khớp với phân bố chuẩn $\mathcal{N}(\hat{\mu}, s^2)$ tốt, giá trị $L(Z_0)$ sẽ cao. Còn không, giá trị $L(Z_0)$ sẽ thấp. Do đó, ta sẽ lựa chọn các điểm POI dựa trên giá trị của $L(Z_0)$. Với mỗi điểm trong một chu kỳ clock, ta tính $L(Z_0)$ cho chúng với cùng các trace đo được và lựa chọn điểm có $L(Z_0)$ lớn nhất là điểm POI. Trong trường hợp một số điểm của giá trị $L(Z_0)$ gần bằng giá trị lớn nhất ta chọn tất cả các điểm đó. Khi đó càng có nhiều điểm xấp xỉ với phân bố chuẩn thì khả năng lập mẫu cho thiết bị càng tốt. Các điểm POI lựa chọn theo đề xuất được thực hiện thông qua thuật toán 1, gọi là thuật toán NDB-POI.

Thuật toán 1: **NDB - POI**

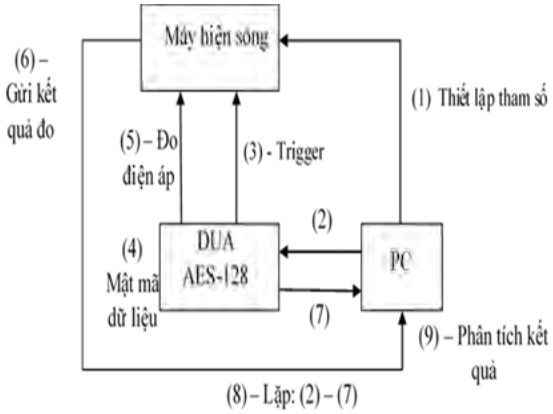
Đầu vào: *Tập trace tương ứng với một class: X gồm N trace, mỗi trace n mẫu, chia làm Nr nhóm.*
Đầu ra: *Các điểm POI:* $(x_1, x_2, \dots, x_m)$.

```
1: SSE = 0;
2: for i=1: Nr-1
      for j = i+1: Nr
          abs = trung bình trace nhóm (j) – trung bình trace nhóm (i);
       SSE = SSE + |abs|
      end
      end
3: Chọn m đỉnh tín hiệu SSE.
4: for i=1: m
      Chọn k điểm xung quanh đỉnh tín hiệu SSE.
       Tính: x_i = arg max_k (1/Nr) Σ_{j=1}^{Nr} L(Z_0)
       Với Z_0 tính theo (10); L(Z_0) tính theo (2);
   end
```

V. THỰC NGHIỆM

A. *Sơ đồ thực nghiệm*

Sơ đồ thí nghiệm tấn công DPA lên AES-128 được thể hiện trên Hình 2.



Hình 2. Sơ đồ thí nghiệm tấn công mẫu lên AES

Trong Hình 2, DUA (Device Under Attack) là thiết bị mật mã cần tấn công. Trong thực nghiệm này đó là một thẻ thông minh có giao diện RS-232 để kết nối với máy tính (PC), thành phần chính trên thẻ thông minh này là một vi điều khiển của hãng ATMEGA8515, thuật toán mật mã được sử dụng trong thực nghiệp là thuật toán AES-128.

Các bước thực hiện như sau:

(1) Sử dụng PC để cấu hình, đặt chế độ cho máy hiện sóng.

(2) PC gửi bản rõ tới DUA và yêu cầu mã hóa.

(3) DUA gửi tín hiệu Trigger tới máy hiện sóng để bắt đầu thực hiện quá trình đo.

(4) DUA thực hiện quá trình mã hóa bản rõ.

(5) Máy hiện sóng thu dạng sóng biểu diễn điện áp thu được tại điểm tấn công.

(6) Máy hiện sóng gửi dữ liệu thu được tới PC để xử lý, phân tích.

(7) DUA gửi bản mã cho PC.

(8) Các bước từ 2 tới 7 được lặp lại với tất cả các bản rõ.

(9) Quá trình phân tích dữ liệu được thực hiện trên PC để tìm ra khóa bí mật.

Chúng tôi, sử dụng sơ đồ đo trên để xây dựng 03 tập trace: Tập A: gồm 50000 trace được đo khi thiết bị thực thi với một khóa gốc cố định và các bản rõ được thay đổi ngẫu nhiên ở mỗi lần đo. Tập B: gồm 50000 trace được đo khi thiết bị thực thi với một khóa gốc cố định giống với tập A và các bản rõ được thay đổi ngẫu nhiên ở mỗi lần đo. Tập C: gồm 100000 trace được đo khi thiết bị thực thi với một khóa gốc cố định khác hai tập trên và các bản rõ được thay đổi ngẫu nhiên ở mỗi lần đo. Tập B, được sử dụng để tìm chỉ số các điểm POI, tập A được sử dụng để xây dựng bộ mẫu của thiết bị và tập C được sử dụng làm tập dữ liệu tấn công. Chúng tôi tiến hành thực hiện 02 thí nghiệm. Thí nghiệm 1 dựa trên tập dữ liệu B để kiểm chứng khả năng phương pháp lựa chọn POI được đề xuất trong bài báo. Thí nghiệm 02: sử dụng tập A, và C để đánh giá hiệu quả của tấn công mẫu với phương pháp lựa chọn POI được đề xuất.

B. *Thí nghiệm 1*

Đối với các thiết bị dựa trên các bộ vi điều khiển, điện năng tiêu thụ rò rỉ theo trọng số Hamming [12], có nghĩa là trọng số Hamming càng lớn thì điện năng tiêu thụ càng lớn hoặc ngược lại. Trọng số Hamming của dữ liệu 1 byte, nhận 9 giá trị $V_i = i; với\ (i = 0,1,2, \dots ,8)$. Với mỗi giá trị trọng số Hamming, lựa chọn 500 trace, và sử dụng thuật toán 1 để xác định các điểm POI. Khi thực hiện thuật toán 1, sau khi có được tín hiệu $SSE(t)$ như thể hiện trên Hình 3, số đỉnh tìm được là $m = 6$. Ứng với mỗi đỉnh ta chọn ra $L = 5$ điểm xung quanh giá trị đỉnh.

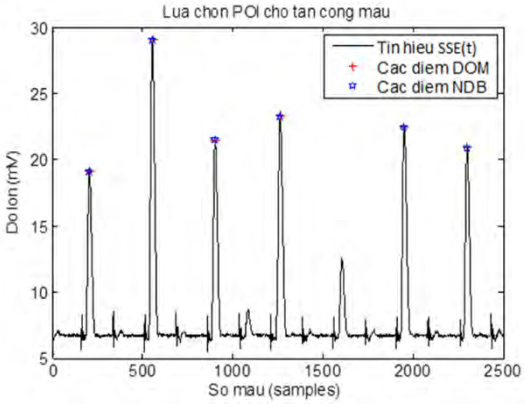
Bảng I. So sánh điểm POI của các phương pháp khác nhau

Chu kỳ clock	1	2	3	4	5	6
NDB	P2	P7	P12	P17	P23	P28
DOM	P3	P7	P13	P16	P22	P27
SNR	P3	P7	P13	P16	P22	P27
CPA	P1	P8	P14	P18	P23	P29
SOSD	P3	P8	P14	P18	P23	P29
SOST	P1	P8	P12	P17	P24	P29

Ứng với mỗi giá trị V_i, chúng ta sẽ sử dụng phương pháp kiểm tra độ khớp để xác định xem phân bố của mẫu quan sát được của các điểm P_i $(i \in \{0,1,2, \dots ,29\})$ có khác với giả sử phân bố lý thuyết $\mathcal{N}(\hat{\mu}, s^2)$ hay không bằng cách tính giá trị $L(Z_0)$ với 500 mẫu. Với giá trị V_i $(i = 0,1,2, \dots ,8)$ và điểm P_j $(j = 0,1,2, \dots ,29)$, ta tính giá trị $L(Z_0)$ và viết lại kết quả thành $L_{i,j}(Z_0)$. Sau đó, chúng ta tính giá trị $L_j(Z_0)$ $(j = 0,1,2, \dots ,29)$ cho từng 30 điểm như sau.

$$L_j(Z_0) = \frac{1}{9}.\sum_{i=0}^{8} L_{i,j}(Z_0), (j = 0,1,2, \dots ,29)$$

Và lựa chọn các điểm POI dựa theo giá trị của $L_0(Z_0), L_1(Z_1), \dots , L_{29}(Z_{29})$. Trong một chu kỳ clock, điểm có giá trị $L_j(Z_0)$ lớn nhất được lựa chọn làm điểm POI. Trong bảng 2, chúng tôi chỉ ra kết quả việc lựa chọn các điểm POI theo một số cách khác nhau từ tập trace B. Từ bảng 2 ta thấy, phương pháp của chúng tôi, NDB cho tìm được các điểm khác với các phương pháp khác. Hình 3 mô tả tín hiệu $SSE(t)$ và các điểm lựa chọn theo phương pháp đề xuất NDB và DOM.



Hình 3. Lựa chọn điểm tấn công

C. *Thí nghiệm 2*

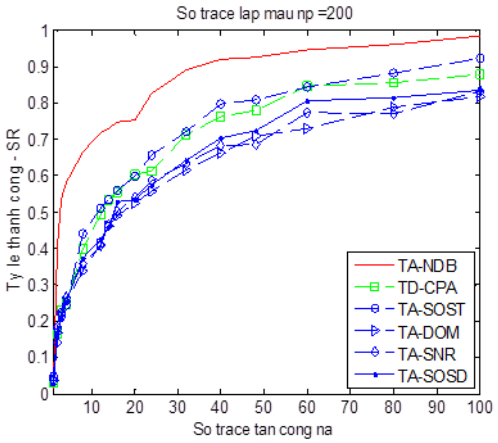
Trong thí nghiệm này chúng tôi thực thi tấn công mẫu đối với tập A để xây dựng mẫu, tập C là tập dữ liệu tấn công bằng cách sử dụng phương pháp lựa chọn POI đề xuất NDB.

Vị trí tấn công AES-128 chúng tôi lựa chọn ở vị trí lối ra của S-hộp vòng thứ nhất. Sử dụng phương pháp tấn công mẫu, chúng tôi xây dựng tập 256 mẫu tương ứng với 256 giá trị của byte tại lối ra S-hộp vòng thứ nhất. Ứng với mỗi giá trị $s_{out} \in \{0,1,2,\dots 255\}$ chúng tôi ghi lại 1000 vết điện năng tiêu thụ, tương ứng với tổng số $256 \times 1000 = 256000$ vết điện năng tiêu thụ, mỗi vết có độ dài 2500 mẫu được thu thập trong khoảng thời gian thiết bị thực thi thao thế S-hộp tại vòng thứ nhất của thuật toán AES-128. Sử dụng phương pháp lựa chọn POI là NDB, khi đó mỗi trace chỉ còn 6 điểm.

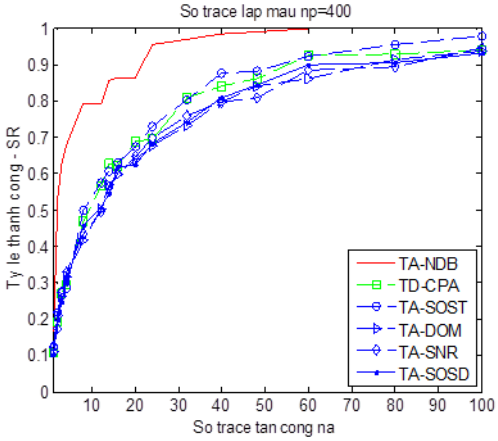
Tham số tỷ lệ thành công, ký hiệu là SR, được đề xuất trong [13] để đánh giá hiệu quả của tấn công TA dựa trên 06 phương pháp lựa chọn POI là NDB, CPA, SOST, DOM, SNR, SOSD lần lượt được ký hiệu là TA-NDB, TA-CPA, TA-SOST, TA-DOM, TA-SNR, TA-SOSD. Tỷ lệ thành công được định nghĩa là tỷ số giữa số lần thí nghiệm khôi phục khóa thành công so với tổng số lần thực hiện thí nghiệm tấn công. Tham số này cho ta biết khả năng thành công của tấn công và giá trị càng gần với 1 là kết quả chúng ta mong muốn. Kết quả thực nghiệm tính giá trị SR cho bởi hình 4 và hình 5 tương ứng với số trace để lập mẫu cho mỗi giá trị bí mật là $n_p = 200$ và $n_p = 400$.

D. *Kết quả thực nghiệm*

Kết quả của thí nghiệm 2 được chỉ ra trên hình 4 và hình 5. Trước hết, khi số trace để lập mẫu tăng từ 200 lên 400 thì hiệu quả của tấn công tăng lên đối với mọi phương pháp lựa chọn các điểm tấn công. Kết quả này có được là bởi khi số trace lập mẫu tăng lên bộ mẫu càng phản ánh chính xác về đặc tính tiêu thụ điện năng của thiết bị. Thứ hai, hiệu quả tấn công mẫu với phương pháp lựa chọn POI dựa trên tính các điểm có phân bố xấp xỉ phân bố chuẩn cho hiệu năng cao hơn cỡ 10%. Với $n_p = 200$, cần cỡ 50 trace để TA_{NDB} có tỷ lệ thành công trên 90%, còn TA_{CPA} và TA_{SOST} là cỡ 80%, còn các phương pháp lựa chọn POI khác cho kết quả nhỏ 80%. Hiệu quả tăng lên rõ rệt khi $n_p = 400$, chỉ cần cỡ 30 trace để TA_{NDB} có tỷ lệ thành công trên 95%. Kết quả thực nghiệm chứng minh hiệu quả của phương pháp lựa chọn POI dựa trên kiểm tra độ khớp phân bố chuẩn của các điểm được lựa chọn. Kết quả này phù hợp với lý thuyết bởi trong tấn công mẫu là các điểm POI có phân bố Gauss chuẩn đa biến, do đó các điểm POI riêng lẻ sẽ tuân theo phân bố chuẩn, được chứng minh bởi bổ đề 2, do đó, khi các điểm POI được lựa chọn có phân bố chuẩn thì khả năng mô xây dựng mẫu của thiết bị càng chính xác. Điều này khiến hiệu quả của việc phân lớp trong pha tấn công tăng lên.



Hình 4. So sánh SR với $n_p = 200$



Hình 5. So sánh SR với $n_p = 400$

VI. KẾT LUẬN

Bài báo trình bày phương pháp mới để lựa chọn các điểm trên trace điện năng tiêu thụ để phục vụ cho tấn công mẫu. Trong phương pháp này, các điểm POI được lựa chọn là những điểm có phân bố xấp xỉ phân bố chuẩn, điều này giúp hiệu quả tấn công mẫu tăng cỡ 10% so với các phương pháp khác. Trong các bài báo tiếp theo chúng tôi sẽ đánh giá hiệu quả của phương pháp lựa chọn POI này kết hợp với một số phương pháp phân lớp khác trong pha tấn công của tấn công mẫu.

TÀI LIỆU THAM KHẢO

[1] Nguyễn Hồng Quang, Phân tích tiêu thụ điện năng của thiết bị

mật mã, Tạp chí Nghiên cứu Khoa học và Công nghệ quân sự, 2014.

[2] Kocher P, Jaffe J, Jun B, Differential Power Analysis, CRYPTO 1999, LNCS 1666. Springer: Heidelberg, pp. 388–397, 1999.

[3] Gandolfi, K., Mourtel, C., Olivier, F, Electromagnetic Analysis: Concrete Results, *CHES2001, LNCS 2162*, pp. 251-261, 2001.

[4] Chari S, Rao JR, Rohatgi P, Template Attacks, CHES 2002, LNCS 2523. Springer: Heidelberg, pp. 13-28, 2002.

[5] Nguyễn Hồng Quang, Trace năng lợng trong DPA, Tạp chí Nghiên cứu Khoa học và Công nghệ quân sự, 2013.

[6] Rechberger C, Oswald E, Practical Template Attacks, WISA 2004, LNCS 3325. Springer: Heidelberg, pp. 440-456, 2004.

[7] Archambeau, C., Peeters, E., Standaert, F.-X., Quisquater, J.-J, Template Attacks in Principal Subspaces, *CHES2006, LNCS 4249*, pp. 1-14, 2006.

[8] B¨ar, M., Drexler, H., Pulkus, Improved Template Attacks, *COSADE2010*, 2010.

[9] B. Gierlichs, K. Lemke, C. Paar, Templates vs. Stochastic Methods, in *CHES*, CHES 2006, pp. 15-29.

[10] S. Mangard, E. Oswald, and T. Popp, Power Analysis Attacks: Revealing the Secrets of Smart Cards. New York: USA: Springer, 2010.

[11] K Pearson, On the criterion that a given system of deviations from the probable in the case of a correlated system of variables is such that it can be reasonably supposed to have arisen from random sampling, Philosophical Magazine, pp. 157-175, 1900.

[12] Brier E, Clavier C, Olivier F, Correlation Power Analysis with a Leakage Model, in CHES 2004, LNCS 3156. Springer: Heidelberg, 2004.

[13] Standaert F-X, Malkin TG, Yung M, A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks, in *EUROCRYPT*, 2009.

[14] Trần Ngọc Quý, Tấn công phân tích điện năng tiêu thụ lên AES-128, Tạp chí Nghiên cứu Khoa học và Công nghệ quân sự, 2015.

[15] Standaert F-X, Archambeau C, Using SubspaceBased Template Attacks to Compare and Combine Power and Electromagnetic Information Leakage, CHES 2008, LNCS 5154. Springer: Heidelberg, pp. 411-425, 2008.

[16] Oswald E, Mangard S, Template Attacks on MasingResistance is Futile, CT- RSA 2007, LNCS 4377. Springer: Heidelberg, pp. 243–256, 2007.

[17] Girelichs B, Batina L, Tuyls P, Preneel B, Mutual Information Analysis, in CHES 2008, LNCS 5154. Springer: Heidelberg, 2004.

[18] Fukunaga K, Introduction to Statistical Pattern Recognition. New York: Elsevier, 1990.

[19] V. Lomné, E. Prouff, and T. Roche, Behind the scene of side channel attacks, in *ASIACRYPT*, 2013.

[20] P.C Kocher, Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, *CRYPTO1996, LNCS 1109*, pp. 104-113, 1996.

[21] European Network of Excellence (ECRYPT). The side channel cryptanalysis lounge. [Online]. http://www.crypto.ruhr-uni-bochum.de/en sclounge.html

[22] Montminy, D.P., Baldwin, R.O., Temple, M.A., Laspe, E.D, Improving crossdevice attacks using zero-mean unit-variance mormalization, Journal of Cryptographic Engineering, vol. 3, no. 2, pp. 99-110, June 2013.

[23] Benedikt Gierlichs, Signal Theoretical Methods in Diff erential Side Channel Cryptanalysis, Ruhr-University of Bochum, Ed.: Diploma Thesis, 2006.

METHOD OF SELECTING ATTACK POINTS FOR PROFILED ATTACK BASED ON NORMAL DISTRIBUTION

Abstract: Profiled attacks are one of the most effective side channel attacks against cryptographic devices. In order to profiled attacks are practical, one must select some attack points on power consumption trace of device. So far, there are many methods to select these points for profiled attacks. However, these selective approaches are based on experience of side channel attacks, and no work hase indicated that these methods of selection are the best. In this paper, we propose a new method of selecting points based on the principle, different from the methods that have been implemented, based on the points which are approximately normal distribution. Verification of results, found that the performance of the attack was significantly improved compared to the current method. Our experiments were done on ATMEGA8515 smartcards installed with AES-128 cryptographic algorithm.

Trần Ngọc Quý, Nhận bằng thạc sỹ Điện tử viễn thông, chuyên ngành Kỹ thuật điện tử và thông tin liên lạc năm 2006 tại trường Đại học Công nghệ - ĐHQGHN. Hiện đang công tác tại Học viện Kỹ thuật Mật mã. Lĩnh vực nghiên cứu: Tấn công kênh kề, tấn công phần cứng, hệ thống nhúng.

Hoàng Văn Quân, Nhận học vị Tiến sỹ năm 2016. Hiện công tác tại Học viện Kỹ thuật Mật mã. Lĩnh vực nghiên cứu: Thiết kế hệ mật, thám mã kênh kề, thám mã lượng sai.

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 ngụy trang cao của các kỹ thuật giấu tin tiên tiến.

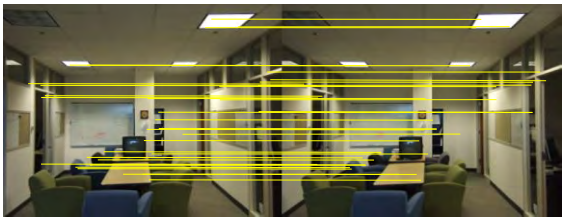
Trong [1], [2] các tác giả đã trình bày phương pháp giấu tin trong miền không gian chủ yếu dùng kỹ thuật LSB. Phương pháp này dễ thực hiện và cũng dễ dàng tấn công và bóc tách thông tin. Trong [3], chúng tôi đã cải tiến thuật toán LSB để tăng tính vô hình cho thông tin mật với sự tham gia của hai pixel 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.

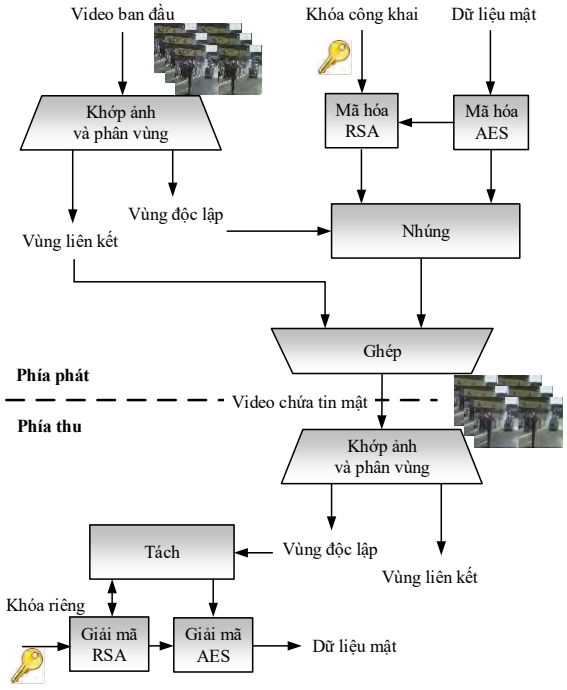
Bảng I. So sánh LSB và LSB kết hợp

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).

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

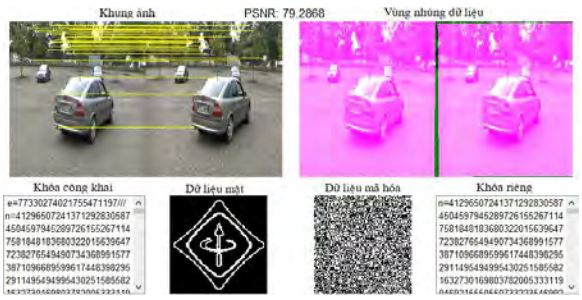
Với: M, N là kích thước khối dữ liệu; $I_{i,j}$ và $I'_{i,j}$ là giá trị của các khối dữ liệu tại điểm i,j.

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

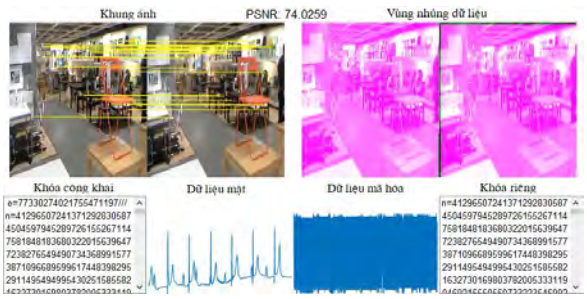
Đối với ảnh 8 bit thì giá trị đỉnh (max) ngõ vào $I_{peak} = 255$.

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.