Tạp chí Tin học và Điều khiển học, T.29, S.3 (2013), 221–231

ĐỒNG BỘ THÍCH NGHI MẠNG CNN HỖN LOẠN VÀ ỨNG DỤNG TRONG BẢO MẬT TRUYỀN THÔNG

ĐÀM THANH PHƯƠNG[1], PHẠM THƯỢNG CÁT[2]

[1] *Trường Đại học Công nghệ thông tin và Truyền thông - Đại học Thái Nguyên.*
Email: dtphuong@ictu.edu.vn

[2] *Viện Công nghệ Thông tin, Viện Hàn lâm Khoa học & Công nghệ Việt Nam.*
Email: ptcat@ioit.ac.vn

Tóm tắt. Bài báo giải quyết bài toán đồng bộ tín hiệu hỗn loạn của một lớp mạng nơ ron tế bào với nhiều tham số chưa biết bằng lý thuyết điều khiển thích nghi. Các thuật điều khiển và luật cập nhật tham số đưa ra được chứng minh đảm bảo tính đồng bộ toàn cục dựa trên lý thuyết ổn định Lyapunov. Trên cơ sở đó, đưa ra mô hình truyền thông bảo mật sử dụng kết quả đồng bộ và đặc tính hỗn loạn của mạng nơron tế bào SC-CNN (State Controlled Cellular Neural Network). Các kết quả tính toán mô phỏng được thực hiện trên Matlab.

Từ khóa. Mạng nơron tế bào, hệ hỗn loạn, đồng bộ thích nghi, bảo mật truyền thông.

Abstract. This paper solves chaotic signal synchronization problem of a cellular neural network with unknown parameters by using adaptive control theory. The constructed control and the parameters update laws are proven to ensure the global synchronization based on Lyapunov stability theory. From this result, we bring out the secure communication model for the synchronization and the chaotic property of the cellular neural network (SC-CNN). The simulation results are performed on Matlab.

Key words. CNN, chaos system, adaptive synchronization, secure communication.

1. GIỚI THIỆU

Nghiên cứu về hành vi hỗn loạn của hệ động học phi tuyến cũng như các ứng dụng của chúng trong các lĩnh vực khác nhau đã thu hút được sự quan tâm nghiên cứu của nhiều nhà khoa học.

Theo hướng nghiên cứu thiết kế các mạch cứng hay các hệ tạo dao động hỗn loạn có thể kể ra kết quả chính như: Hệ hỗn loạn Lorenz [6], hệ hỗn loạn Chen [7], hệ hỗn loạn thống nhất [8] hay các mạch Chua, Lure trên cơ sở lý thuyết mạng nơron tế bào [10, 13].

Theo hướng ứng dụng hỗn loạn, sau khi Pecora và Carroll đưa ra khái niệm đồng bộ drive – response [12], đã có nhiều mô hình truyền thông bảo mật sử dụng đồng bộ hỗn loạn được đề xuất [3, 5, 9, 16, 17]. Tư tưởng chung của các mô hình này là áp dụng bài toán đồng bộ để bên nhận có thể tự xây dựng được dòng khoá mật dùng để giải mã. Theo hướng ứng dụng này, để giải quyết bài toán đồng bộ drive – response hai mạng nơron tế bào SC-CNN với các tham số

không chắc chắn và tín hiệu quan sát được của hệ drive không đầy đủ. Mô hình truyền thông bảo mật ảnh sử dụng kết quả đồng bộ này cũng được đưa ra. Kết quả lý thuyết được chứng minh bằng lý thuyết ổn định Lyapunov, hiện quả của thuật toán mã hoá được kiểm chứng thông qua các độ đo phổ biến trong mã hoá ảnh.

Sau phần giới thiệu, Mục 2 mô tả về mô hình SC-CNN được sử dụng. Mục 3 tập trung thiết kế bộ điều khiển thích nghi và luật cập nhật tham số ước lượng giải quyết bài toán đồng bộ hai hệ hỗn loạn với nhiều tham số chưa biết. Mục 4 trình bày mô hình truyền thông bảo mật đề xuất và các phân tích, đánh giá. Cuối cùng là phần kết luận.

2. MÔ HÌNH SC-CNN

Ngoài mô hình gốc của Leon Chua và LingYang [10], CNN còn được phát biểu dưới nhiều mô hình khác như mô hình SC-CNN (State controlled CNN) [14]; mô hình Full range CNN [2]; mô hình Reaction – diffusion CNN [2]... Theo [14], phương trình trạng thái của SC-CNN tổng quát viết cho mỗi cell như sau

$$\dot{x}_j = -x_j + \sum_{C(k)\in N(j)} A_{j,k}y_k + \sum_{C(k)\in N(j)} B_{j,k}u_k + \sum_{C(k)\in N(j)} C_{j,k}x_k + I_j \tag{1}$$

với j là chỉ số cells, x_j là biến trạng thái và y_j là hàm đầu ra của cell được định nghĩa bởi hàm tuyến tính từng đoạn

$$y_j = f(x_j) = \frac{1}{2}\left(|x_j + 1| - |x_j - 1|\right), \tag{2}$$

$N(j)$ là tập lân cận của cell $C(j)$, I_j là giá trị ngưỡng. Các hằng số $A_{j,k}$, $B_{j,k}$, $C_{j,k}$ lần lượt là các ma trận trọng số liên kết phản hồi, điều khiển và mẫu.

Với SC-CNN 3 cells phương trình (1) (2) được viết tường minh như sau

$$\begin{cases} \dot{x}_1 = -x_1 + \sum\limits_{k=1}^{3} a_{1k}y_k + \sum\limits_{k=1}^{3} s_{1k}x_k + i_1 \\ \dot{x}_2 = -x_2 + \sum\limits_{k=1}^{3} a_{2k}y_k + \sum\limits_{k=1}^{3} s_{2k}x_k + i_2 \\ \dot{x}_3 = -x_3 + \sum\limits_{k=1}^{3} a_{3k}y_k + \sum\limits_{k=1}^{3} s_{3k}x_k + i_3 \end{cases} \tag{3}$$

Để thực hiện mạch mạng SC-CNN theo cấu trúc mạch Chua kinh điển [11], theo [15] tác giả đã lựa chọn các tham số phù hợp để phương trình (3) trở thành

$$\begin{cases} \dot{x}_1 = -x_1 + a_{11}y_1 + s_{11}x_1 + s_{13}x_3 \\ \dot{x}_2 = -x_2 + s_{22}x_2 + s_{23}x_3 \\ \dot{x}_3 = -x_3 + s_{31}x_1 + s_{32}x_2 + s_{33}x_3 \end{cases} \tag{4}$$

Với việc đặt

$$a_{11} = \alpha_1(b - a); s_{11} = (1 - \alpha_1 b); s_{13} = \alpha_1; s_{22} = (1 + \alpha_2);$$
$$s_{23} = -1; s_{31} = -\beta; s_{32} = \beta; s_{33} = (1 - \beta)$$

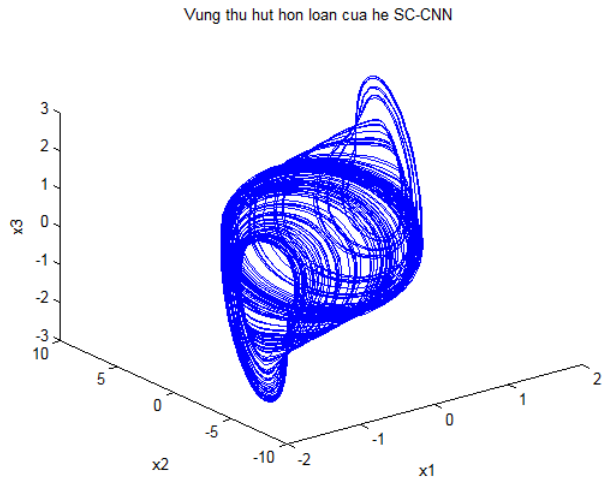
ta có thể thấy phương trình (4) tương đương với phương trình Chua kinh điển

$$\begin{cases} \dot{x} = \alpha_1 (z - h(x)) \\ \dot{y} = \alpha_2 y - z \\ \dot{z} = \beta (y - x - z) \\ h(x) = bx + 0.5 (a - b) (|x + 1| - |x - 1|) \end{cases} \tag{5}$$

Việc nghiên cứu tính chất động học của (4) phụ thuộc vào các tham số đã được trình bày chi tiết trong [15]. Chẳng hạn với bộ tham số $s_{11} = -1.2418$, $s_{13} = 0.3050$, $s_{22} = 1.4725$, $s_{23} = -1.0000$, $s_{31} = -0.3143$, $s_{32} = 0.3143$, $s_{33} = 0.6857$, $a_{11} = 2.2754$ ta nhận được giá trị riêng của ma trận ổn định

$$J_0 = \begin{bmatrix} s_{11} + a_{11} - 1 & 0 & s_{13} \\ 0 & s_{22} - 1 & s_{23} \\ s_{31} & s_{32} & s_{33} - 1 \end{bmatrix}$$

lần lượt là $\lambda_1 = 0.1907$, $\lambda_2 = 0.0006 + i\,(0.5166)$ $\lambda_3 = 0.0006 - i\,(0.5166)$ và hệ (4) là hệ hỗn loạn. Hình 1 mô tả vùng thu hút hỗn loạn double scroll của hệ (4) với các tham số này, thực hiện trên Matlab.



Hình 1. Vùng thu hút hỗn loạn của hệ SC-CNN mô phỏng trên Matlab

3. BÀI TOÁN ĐỒNG BỘ THÍCH NGHI

3.1. Mô tả và giải quyết bài toán

Bài toán đồng bộ drive – response được Pecora và Carroll đề xuất năm 1990 [12]. Mục đích của bài toán là điều khiển hệ response sao cho tín hiệu (trạng thái hoặc đầu ra) của hệ response đồng bộ với tín hiệu tương ứng của hệ drive. Trong phần này của bài báo sẽ giải quyết bài toán đồng bộ drive – response hai hệ SC-CNN có cùng cấu trúc bằng thuật điều khiển thích nghi. Với giả thiết một số tham số hệ thống không được biết đối với hệ response

và chỉ quan sát được một phần tín hiệu của hệ drive, luật điều khiển thích nghi được thiết kế đảm bảo hai hệ đồng bộ tiệm cận toàn cục và xác định được tham số thực của hệ response.

Xét hệ hỗn loạn drive SC-CNN

$$\begin{cases} \dot{x}_{1d} = -x_{1d} + a_{11}y_{1d} + s_{11}x_{1d} + s_{13}x_{3d} \\ \dot{x}_{2d} = -x_{2d} + s_{22}x_{2d} + s_{23}x_{3d} \\ \dot{x}_{3d} = -x_{3d} + s_{31}x_{1d} + s_{32}x_{2d} + s_{33}x_{3d} \end{cases} \tag{6}$$

với $a_{11}, s_{11}, s_{22}, s_{33}, s_{13}, s_{23}, s_{31}, s_{32}$ là các hằng số đã biết, được lựa chọn để đảm bảo (6) là hệ hỗn loạn. Giả sử các tham số s_{13}, s_{23} là hoàn toàn chưa biết đối với hệ response. Khi đó hệ response được xác định như sau

$$\begin{cases} \dot{x}_{1r} = -x_{1r} + a_{11}y_{1r} + s_{11}x_{1r} + \hat{s}_{13}x_{3r} + u_1 \\ \dot{x}_{2r} = -x_{2r} + s_{22}x_{2r} + \hat{s}_{23}x_{3r} + u_2 \\ \dot{x}_{3r} = -x_{3r} + s_{31}x_{1r} + s_{32}x_{2r} + s_{33}x_{3r} + u_3 \end{cases} \tag{7}$$

trong đó $\hat{s}_{13}, \hat{s}_{23}$ là các hàm ước lượng tham số theo thời gian t và u_1, u_2, u_3 là các hàm điều khiển. Các chỉ số dưới d, r ký hiệu hệ drive và response tương ứng. Trừ (7) cho (6) ta được hệ động học lỗi

$$\begin{cases} \dot{e}_1 = -e_1 + a_{11}\left(y_{1r} - y_{1\mathrm{d}}\right) + s_{11}e_1 + \left(\hat{s}_{13} - s_{13}\right)x_{3r} + s_{13}e_3 + u_1 \\ \dot{e}_2 = -e_2 + s_{22}e_2 + \left(\hat{s}_{23} - s_{23}\right)x_{3r} + s_{23}e_3 + u_2 \\ \dot{e}_3 = -e_3 + s_{31}e_1 + s_{32}e_2 + s_{33}e_3 + u_3 \end{cases} \tag{8}$$

Với giả thiết hệ response chỉ có được một phần tín hiệu $\mathbf{s} = (x_{1\mathrm{d}}, x_{2\mathrm{d}})^T$ của hệ driver, bộ điều khiển và luật cập nhật tham số được thiết kế như sau

$$\begin{array}{l} u_1 = -a_{11}\left(y_{1r} - y_{1\mathrm{d}}\right) - k_1e_1; u_2 = -k_2e_2; u_3 = 0; k_i = {e_i}^2\,(i = 1, 2)\,; \\ \dot{\hat{s}}_{13} = -e_1x_{3\mathrm{r}}; \dot{\hat{s}}_{23} = -e_2x_{3\mathrm{r}} \end{array}. \tag{9}$$

Định lý 1. *Hai hệ hỗn loạn SC-CNN (6), (7) đồng bộ tiệm cận toàn cục với bộ điều khiển và luật cập nhật tham số (9).*

Chứng minh. Lựa chọn hàm Lyapunov

$$V\left(\mathbf{e}(t)\right) = \frac{1}{2}({e_1}^2 + {e_2}^2 + {e_3}^2 + \left(\hat{s}_{13} - s_{13}\right)^2 + \left(\hat{s}_{23} - s_{23}\right)^2 + \left(k_1 - l_1\right)^2 + \left(k_2 - l_2\right)^2) \tag{10}$$

trong đó $\mathbf{e}(t) = (e_1, e_2, e_3)^T$ là véc tơ sai lệch trạng thái giữa hệ drive (6) và response (7); l_1, l_2 là các hằng số xác định, sẽ được lựa chọn sau.

Đạo hàm (10) theo thời gian, sử dụng (8), (9) ta thu được

$$\begin{array}{l} \dot{V}\left(\mathbf{e}(t)\right) = e_1\dot{e}_1 + e_2\dot{e}_2 + e_3\dot{e}_3 + \left(\hat{s}_{13} - s_{13}\right)\dot{\hat{s}}_{13} + \left(\hat{s}_{23} - s_{23}\right)\dot{\hat{s}}_{23} + \left(k_1 - l_1\right)\dot{k}_1 + \left(k_2 - l_2\right)\dot{k}_2 \\ = \left(-{e_1}^2 + s_{11}{e_1}^2 + \left(\hat{s}_{13} - s_{13}\right)e_1x_{3r} + s_{13}e_1e_3 - k_1{e_1}^2\right) \\ + \left(-{e_2}^2 + s_{22}{e_2}^2 + \left(\hat{s}_{23} - s_{23}\right)e_2x_{3r} + s_{23}e_2e_3 - k_2{e_2}^2\right) \\ + \left(-{e_3}^2 + s_{31}e_1e_3 + s_{32}e_2e_3 + s_{33}{e_3}^2\right) - \left(\hat{s}_{13} - s_{13}\right)e_1x_{3r} \\ - \left(\hat{s}_{23} - s_{23}\right)e_2x_{3r} + \left(k_1 - l_1\right){e_1}^2 + \left(k_2 - l_2\right){e_2}^2 \\ = {e_1}^2\left(-1 + s_{11} - l_1\right) + {e_2}^2\left(-1 + s_{22} - l_2\right) + {e_3}^2\left(-1 + s_{33}\right) + e_1e_3\left(s_{13} + s_{31}\right) + e_2e_3\left(s_{23} + s_{32}\right) \end{array}.$$

Theo bất đẳng thức cosi, ta có

$$e_1 e_3 \left(s_{13} + s_{31}\right) \leq \frac{1}{2} {e_1}^2 + \frac{1}{2} {e_3}^2 (s_{13} + s_{31})^2,$$

$$e_2 e_3 \left(s_{23} + s_{32}\right) \leq \frac{1}{2} {e_2}^2 + \frac{1}{2} {e_3}^2 (s_{23} + s_{32})^2.$$

Từ đó ta được

$$\begin{array}{l} \dot{V}\left(\mathbf{e}(t)\right) \leq {e_1}^2 \left(-1 + s_{11} - l_1 + \frac{1}{2}\right) + {e_2}^2 \left(-1 + s_{22} - l_2 + \frac{1}{2}\right) \\ + {e_3}^2 \left(-1 + s_{33} + \frac{1}{2}(s_{13} + s_{31})^2 + \frac{1}{2}(s_{23} + s_{32})^2\right) \end{array}.$$

Chọn $l_1 = s_{11} + \frac{1}{2}; l_2 = s_{22} + \frac{1}{2}$ và với chú ý khi lựa chọn tham số cho hệ hỗn loạn (6) phải thoả mãn

$$s_{33} + \frac{1}{2}(s_{13} + s_{31})^2 + \frac{1}{2}(s_{23} + s_{32})^2 \leq 1 - \varepsilon; \varepsilon > 0, \tag{11}$$

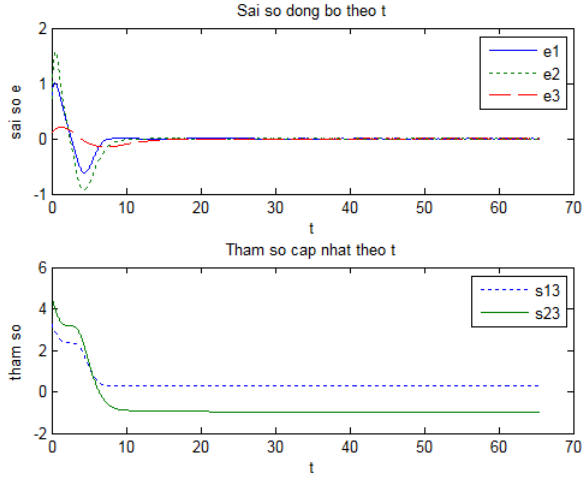
ta có,

$$\dot{V}\left(\mathbf{e}(t)\right) \leq -{e_1}^2 - {e_2}^2 - \varepsilon {e_3}^2 < 0. \tag{12}$$

Theo lý thuyết ổn định Lyapunov, từ (12) cho thấy $\lim\limits_{t \to \infty} e_i = 0;\ i = 1, 2, 3$. Hay hệ (7) đồng bộ tiệm cận toàn cục với hệ (6). ■

3.2. Mô phỏng

Để thấy được hiệu quả đồng bộ, ta tiến hành mô phỏng với Matlab R2012a. Các tham số chuẩn bị mô phỏng được chọn như sau



Hình 2. Sai số đồng bộ và tham số ước lượng theo thời gian

Chọn các giá trị tham số đảm bảo hệ driver (6) là hệ hỗn loạn

$$\begin{array}{l} a_{11} = 2.2754, s_{11} = -1.2418, s_{13} = 0.3050, s_{22} = 1.4725 \\ s_{23} = -1.0000, s_{31} = -0.3143, s_{32} = 0.3143, s_{33} = 0.6875 \end{array}. \tag{13}$$

Ta có $s_{33}+\frac{1}{2}(s_{13}+s_{31})^2+\frac{1}{2}(s_{23}+s_{32})^2=0.9226\leq 1-\varepsilon;\varepsilon>0$, thoả mãn điều kiện (11)

Giá trị ban đầu của hệ driver (6): $\mathbf{x}_d(0)=(-0.4532,-0.2137,0.6092)^T$.
Giá trị ban đầu của hệ response (7): $\mathbf{x}_r(0)=(0.3248,0.5121,0.7321)^T$.
Giá trị ban đầu của các tham số ước lượng $\hat{s}_{13},\hat{s}_{23}$: $\theta=(3.2306,4.4312)^T$.
Giá trị ban đầu của bộ tham số điều khiển k_1,k_2: $\mathbf{k}(0)=(-0.8145,1.5315)^T$.
Số nút lưới thời gian là $\Delta t=0.001, t=(256\times 256+1)\times\Delta t$.
Bộ điều khiển và luật cập nhật tham số theo (9).

Kết quả đồng bộ được thể hiện trong hình 2. Ta thấy, các sai số trạng thái giữa hệ response và hệ driver hội tụ về 0, các tham số ước lượng của hệ response hội tụ về tham số thật của hệ driver: Tham số $\hat{s}_{13}$ hội tụ về 0.305; tham số $\hat{s}_{23}$ hội tụ về -1.

4. MÔ HÌNH TRUYỀN THÔNG BẢO MẬT DÙNG ĐỒNG BỘ HỖN LOẠN

4.1. Mô tả mô hình đề xuất

Theo kết quả giải quyết bài toán đồng bộ hỗn loạn trình bày ở trên, ta thấy hệ drive (6) chỉ cần truyền phần tín hiệu $\mathbf{s}=(x_{1\mathrm{d}},x_{2\mathrm{d}})^T$ cho hệ response, hai hệ vẫn thoả mãn đồng bộ tiệm cận toàn cục thông qua bộ điều khiển và luật cập nhật tham số (9). Hơn nữa, các tham số ước lượng của hệ response cũng hội tụ về tham số thực không được biết của hệ drive. Dựa trên các kết quả này, có thể đề xuất lược đồ truyền thông bảo mật ảnh được mô tả chi tiết như sau.

Quá trình mã hoá

Bước 1: Chuyển ma trận pixel ảnh về chuỗi pixel một chiều
Ảnh rõ được tiền xử lý để trở thành một chuỗi tín hiệu $s_i;i=1,...,m.n$, trong đó m,n là kích thước của ảnh. Quá trình này tách ma trận ảnh $A=(a_{ij})_{m\times n}$ theo thứ tự từ trên xuống dưới, từ trái sang phải

$$s_1=a_{11},s_2=a_{12},...,s_n=a_{1n},...,s_{(m-1)n}=a_{m1},s_{(m-1)n+1}=a_{m2},...,s_{mn}=a_{mn}. \quad (14)$$

Bước 2: Khởi tạo các giá trị ban đầu cho hệ drive
Thiết lập giá trị ban đầu $\mathbf{x}_{\mathrm{d}}(0)=(x_{01},x_{02},x_{03})^T$ và bộ tham số hỗn loạn cho hệ drive. Hai bên thống nhất một thời gian trễ t_0 để hai hệ hỗn loạn có thể đồng bộ được. Số nút lưới thời gian để giải hệ SC-CNN (6) là $t=t_0+mn$.

Bước 3: Tạo chuỗi khoá
Với $t_0\leq t_s\leq mn$, khoá mã của mô hình đề xuất là

$$K=(x_{01},x_{02},x_{03},s_{13},s_{23},t_s). \quad (15)$$

$$A=100\left(|x_{1\mathrm{d}}(t_s)|+|x_{2\mathrm{d}}(t_s)|+|x_{3\mathrm{d}}(t_s)|\right);B=100\left(|s_{13}|+|s_{23}|\right) \quad (16)$$

$$k_i=\mathrm{mod}\left(floor\left(A\times|x_{3d}(j)|+B\right),2^b\right);j=t_0+1,..,mn;i=1,...,mn. \quad (17)$$

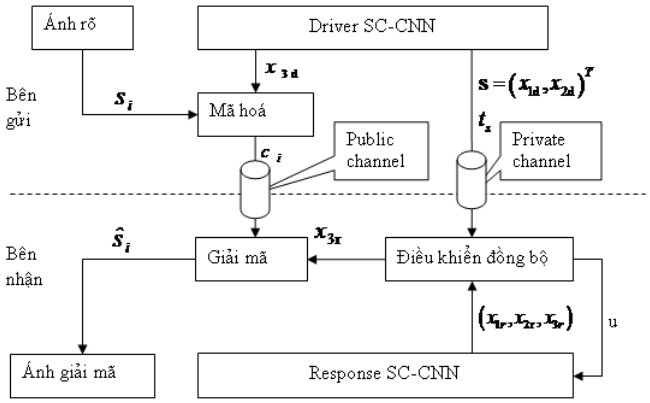
Bước 4: Mã hoá

$$s_i=de2bi(s_i,b),k_i=de2bi(k_i,b);i=1,2,...,mn. \quad (18)$$

$$c_i = bitxor\left(s_i, k_i\right); i = 1, 2, ..., mn \tag{19}$$

trong đó hàm mod (x, y) trả về phần dư của phép chia số nguyên x cho số nguyên y; hàm $floor(x)$ trả về giá trị nguyên gần x nhất nhỏ hơn x (làm tròn dưới); b là số bit biểu diễn ảnh. Hàm $de2bi(a, b)$ thực hiện chuyển số nguyên dương a về số nhị phân b bit; hàm $bitxor(s, k)$ thực hiện phép toán XOR bit hai số nhị phân s, k.

Sau khi mã hoá, chuỗi tín hiệu c_i được truyền cho bên nhận qua kênh truyền tin công cộng. Tín hiệu điều khiển $\mathbf{s} = (x_{1\mathrm{d}}, x_{2\mathrm{d}})^T$ và thành phần t_s của khoá được gửi cho bên nhận qua kênh truyền tin mật. Thực hiện đồng bộ hệ (7) theo luật điều khiển (9) để có được các tín hiệu phục vụ giải mã.



Hình 3. Mô hình truyền thông bảo mật ảnh đề xuất

Quá trình giải mã

Bước 1: Tính toán các tham số khoá ước lượng

$$\hat{A} = 100\left(\left|x_{1r}\left(t_s\right)\right| + \left|x_{2\mathrm{r}}\left(t_s\right)\right| + \left|x_{3\mathrm{r}}\left(t_s\right)\right|\right); \hat{B} = 100\left(\left|\hat{s}_{13}\right| + \left|\hat{s}_{23}\right|\right). \tag{20}$$

$$\hat{k}_i = \mathrm{mod}\left(floor\left(\hat{A} \times \left|x_{3r}\left(j\right)\right| + \hat{B}\right), 2^b\right); j = t_0 + 1, .., mn; i = 1, ..., mn. \tag{21}$$

Bước 2: Giải mã

$$\hat{k}_i = de2bi\left(\hat{k}_i, b\right); i = 1, 2, ..., mn. \tag{22}$$

$$\hat{s}_i = bitxor\left(c_i, \hat{k}_i\right); i = 1, 2, ..., mn. \tag{23}$$

Bước 3: Khôi phục lại ảnh giải mã

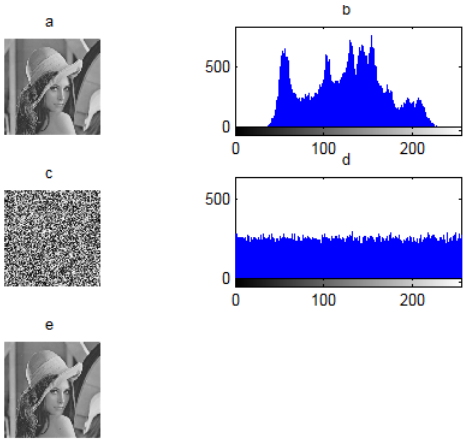
$$\hat{s}_i = \mathrm{bi2}de\left(\hat{s}_i\right); i = 1, 2, ..., mn. \tag{24}$$

Khôi phục lại ma trận ảnh từ chuỗi s_i theo thứ tự từ dưới lên trên, từ phải sang trái.

Theo kết quả bài toán đồng bộ đã giải quyết ở phần trên, cùng với điều kiện bên nhận biết thành phần t_s của khoá K để tính $\hat{A}$, dễ thấy mô hình đảm bảo khôi phục được ảnh gốc từ ảnh mã. Hình 3 mô tả lược đồ truyền ảnh bảo mật đề xuất.

4.2. Mô phỏng và phân tích bảo mật

Các giá trị ban đầu chuẩn bị cho quá trình đồng bộ được lựa chọn như Mục 3.2. Thời gian trễ $t_0 = 1$s. Khoá mã $K = (-0.4532, -0.2137, 0.6092, 0.305, -1, 10)$. Ảnh gốc được lựa chọn là ảnh Lena 8 bit, đa mức xám, kích thước 256×256; Kết quả mã hoá và giải mã sử dụng mô hình đề xuất được thể hiện trong hình 4.



Hình 4. Kết quả mã hoá và giải mã: a. Ảnh gốc Lena, b. Histogram của ảnh gốc, c. Ảnh mã, d. Histogram của ảnh mã, e. Ảnh giải mã

Để phân tích độ bảo mật của mô hình, ta nhắc lại khái niệm một số độ đo thường được sử dụng để phân tích hiệu quả của thuật toán mã hoá ảnh sau.

Định nghĩa 1. [1] Biểu đồ Histogram của ảnh là một dạng biểu đồ mô tả sự phân bố của các giá trị mức xám của các điểm ảnh trong vùng ảnh số. Histogram của một ảnh số với mức xám thuộc độ dài xám $[0, L-1]$ là $h(r_k) = n_k$ với r_k là mức xám thứ k, n_k là số điểm ảnh có cùng mức xám k. Xác suất của mức xám $p(r_k) = \frac{n_k}{n}$ với n là tổng số điểm ảnh.

Định nghĩa 2. [4] Nếu một sự kiện ngẫu nhiên rời rạc x có thể nhận các giá trị là $m_1, m_2, ..., m_n$ thì Entropy của nó là

$$H(m) = -\sum_{i=1}^{n} p(m_i)\log_2 p(m_i)$$

với $p(m_i)$ là xác suất xảy ra của giá trị m_i.

Độ đo thông tin Entropy phản ánh lượng tin trung bình và độ bất ngờ của nguồn tin. Với ảnh 8 bit ta có $m_i = 0, 1, ..., 255; n = 256$. Đối với ảnh 8 bit hoàn toàn ngẫu nhiên thì xác suất xuất hiện các giá trị mức xám là bằng nhau và bằng $\frac{1}{256}$, hay Entropy lý tưởng của ảnh hoàn toàn ngẫu nhiên là $H(m) = -\sum_{i=1}^{256} \frac{1}{256}\log_2 \frac{1}{256} = 8$.

Định nghĩa 3. [18] Gọi C^1, C^2 lần lượt là ảnh mã trước khi và sau khi có một pixel thay đổi ở ảnh gốc. Giá trị pixel tại điểm (i, j) trong C^1, C^2 được ký hiệu là $C^1(i, j), C^2(i, j)$. Khi đó NPCR (Number of Pixels Change Rate) và UACI (Unified Averaged Changed Intensity) được

xác định như sau

$$NPCR : N\left(C^1, C^2\right) = \sum_{i,j} \frac{D\left(i,j\right)}{m \times n} \times 100\%$$

$$UACI : U\left(C^1, C^2\right) = \frac{1}{m \times n} \sum_{i,j} \frac{\left|C^1\left(i,j\right) - C^2\left(i,j\right)\right|}{255} \times 100\%$$

trong đó $D\left(i,j\right) = \begin{cases} 0 & C^1\left(i,j\right) = C^2\left(i,j\right) \\ 1 & C^1\left(i,j\right) \neq C^2\left(i,j\right) \end{cases}$

NPCR và UACI là hai độ đo sự nhạy cảm của hệ mã với những thay đổi nhỏ của ảnh gốc và khoá. NPCR thể hiện số phần trăm pixel khác nhau của hai ảnh. UACI thể hiện cường độ thay đổi trung bình thống nhất giữa hai ảnh. Giá trị lý tưởng của NPCR là 100%, của UACI là 33.33% [18]. Tuy nhiên điều này hiếm khi xảy ra kể cả với hai ảnh hoàn toàn ngẫu nhiên. Các thuật toán đề xuất đều mong muốn các độ đo này càng gần giá trị lý tưởng càng tốt.

Phân tích bảo mật

Đối với mô hình đề xuất ta có các kết quả sau.

Thứ nhất, ta thấy rằng biểu đồ Histogram của ảnh mã có phân bố gần như đồng đều thể hiện trong hình 4, chứng tỏ ảnh gốc đã được mã hoá tốt.

Thứ 2, tính toán Entropy của ảnh gốc ta được $H_1 = 7.3441$. Trong khi Entropy của ảnh mã tương ứng là $H_2 = 7.9972$, rất gần giá trị lý tưởng $H = 8$. Điều này có nghĩa là ảnh mã gần như một nguồn ngẫu nhiên và khả năng rò rỉ thông tin trong quá trình mã hoá là không đáng kể. Nói cách khác, mô hình đề xuất đảm bảo chống lại được kiểu tấn công Entropy.

Thứ 3, kiểm tra sự nhạy cảm của hệ mã với những thay đổi nhỏ của khoá. Giả sử bên thứ 3 có được khoá mã hoá $L = \left(x_{01} + 10^{-10}, x_{02} + 10^{-10}, x_{03} + 10^{-10}, s_{13}, s_{23}, t_s\right)$ để mã hoá và giải mã với sai số 10^{-10} ở ba thành phần đầu. Tính toán ta được NPCR=99.6185% và UACI =28.13%. Tương tự, khi các tham số khác của hệ drive thay đổi với sai số 10^{-10} ta đều thu được NPCR và UACI xung quanh giá trị trên. Các kết quả này cho thấy thuật toán mã hoá đề xuất rất nhạy cảm với khoá và ảnh rõ. Điều này giúp chống lại các tấn công biết bản rõ, là loại tấn công mà thông qua đó bên tấn công có thể tìm ra mối liên hệ có ý nghĩa giữa ảnh gốc và ảnh được mã hoá. Hình 5 thể hiện kết quả giải mã bằng khoá L.

Hình 5. Kết quả giải mã khi có một sự thay đổi nhỏ của khoá, a. Ảnh mã hoá bằng khoá K, b. Ảnh giải mã theo thuật toán đề xuất, c. Ảnh giải mã bằng khoá L.

Thứ 4, về không gian khoá, hệ SC-CNN (6) ứng dụng trong mô hình có 8 tham số hệ thống tác động vào quá trình sinh hỗn loạn và trực tiếp làm ảnh hưởng đến tín hiệu đầu ra của hệ drive và response. Thêm vào đó là 3 tham số giá trị ban đầu của hệ drive tham gia

trực tiếp vào khoá. Độ nhạy cảm đã được kiểm chứng của 11 tham số này là 10^{-10}. Ngoài ra, theo (15) thành phần khoá t_s nhận giá trị trong khoảng $(t_0, 256 \times 256)$. Vì vậy không gian khoá vào khoảng $10^{110} \times 65000 \approx 2^{381}$. Không gian khoá là đủ lớn để chống lại các tấn công dò khoá.

Từ các phân tích trên có thể khẳng định, mô hình đề xuất đảm bảo hiệu quả bảo mật.

4.3. So sánh với một số thuật toán mã hoá ảnh dựa trên hỗn loạn khác

Để đánh giá tổng quan, ta tiến hành so sánh với các thuật toán mã hoá hỗn loạn khác được công bố gần đây. Bảng 1 thể hiện kết quả so sánh các độ đo phổ biến của mô hình đề xuất với các thuật toán của Rhouma [16], Behnia, [3], J.Peng [9], và C. Cheng [5].

Bảng 1. Kết quả so sánh với một số thuật toán mã hoá hỗn loạn khác

	Các thuật toán mã hoá				
Các giá trị so sánh	Rhouma (2008)	Behnia (2008)	J. Peng (2009)	C. Cheng (2013)	Mô hình đề xuất
Entropy	7.9732	7.9968	7.9969	7.9765	7.9972
NPCR	99.58%	41.96%	99.65%	99.62%	99.62%
UACI	33.38%	33.28%	33.46%	33.40%	28.13%
Key space	2^{192}	2^{260}	2^{314}	2^{398}	2^{381}

Ta thấy, mô hình đề xuất có Entropy tốt hơn cả so với 4 thuật toán còn lại. Giá trị NPCR thấp hơn thuật toán của J. Peng. Tuy nhiên, việc mã hoá và giải mã của J. Peng lại sử dụng chung một CNN xác định [9]. Để giải mã được cần đầy đủ thông tin về khoá chứ không có quá trình đồng bộ thích nghi để tự xác định lại khoá như mô hình đề xuất. Về không gian khoá, mô hình đề xuất có không gian khoá lớn thứ 2, sau thuật toán của C. Cheng. Sở dĩ thuật toán này có không gian khoá lớn là do việc mã hoá dựa trên đồng bộ hai hệ hỗn loạn có cấu trúc hoàn toàn khác nhau (Hệ hỗn loạn thống nhất - unified chaotic systems và CNN). Tuy nhiên, để đồng bộ được hệ drive phải gửi đầy đủ 3 tín hiệu trạng thái điều khiển cho hệ response [5]. Điều này bất lợi hơn so với mô hình đề xuất chỉ gửi 2 trên 3 tín hiệu trạng thái. Về giá trị UACI, thuật toán đề xuất có giá trị thấp nhất. Do việc tạo dòng khoá (17) chỉ phụ thuộc 1 tín hiệu hỗn loạn để đơn giản trong tính toán nên chưa tận dụng hết được khả năng hoà trộn của hệ hỗn loạn CNN.

Xét một cách tổng thể, có thể đánh giá mô hình đề xuất có hiệu quả tương đương với các mô hình so sánh.

5. KẾT LUẬN

Bài báo đã giải quyết bài toán đồng bộ hỗn loạn hai mạng SC-CNN. Các kết quả đã được chứng minh chặt chẽ theo lý thuyết ổn định Lyapunov. Trên cơ sở đó đã đưa ra mô hình truyền thông ảnh bảo mật sử dụng đồng bộ hỗn loạn. Quá trình phân tích bảo mật cho thấy mô hình đảm bảo chống lại được một số kiểu tấn công. Trong tương lai, chúng tôi sẽ tiếp tục cải tiến nâng cao hiệu quả của thuật toán và tiến hành thực hiện mạch bài toán đồng bộ mạng SC-CNN.

TÀI LIỆU THAM KHẢO

[1] Rafael C. Gonzalez, Richard E. Woods, *Digital Image Processing*, third edition, Pearson Prentical Hall, 2008.

[2] A.Rodriguez, S. Espejo, R. Dominguez, et all., A Current - model cellular neural network, *IEEE Trans. Circuit and Systems – II* **40** (3) (1993) 147–155.

[3] S. Behnia, A. Akhshani, H. Mahmodi, A novel algorithm for image encryption based on mixture of chaotic map, *Chaos, Solitons and Fractals* **35** (2008) 408–419.

[4] C.E. Shannon, A mathematical theory of communication, *Bell System Technical Journal* **27** (1948) 379 – 423.

[5] C. Cheng and C. Bin Cheng, An asymmetric image cryptosystem based on the adaptive synchronization of an uncertain unified chaotic system and a cellular neural network, *Commun Nonlinear Sci Numer Simulat* **18** (2013) 2825–2837.

[6] E. N. Lozenz, Deteministic nonperiodic flow, *J. Atmos. Sci* **20** (1963) 130–141.

[7] G. Chen and T. Ueta, Yet another chaotic atractor, *International Journal of Bifurcation and Chaos* **9** (1999) 1465–1466.

[8] J. Lu and G. Chen, A new chaotic atractor coined, *International Journal of Bifurcation and Chaos* **12** (2002) 659–661.

[9] Jun Peng and Du Zhang, Image encryption and chaotic cellular neural network, *Machine Learning in Cyber Trust, Chapter 8*, Springer, 2009.

[10] L. Chua and L. Yang, Cellular neural networks: theory, *IEEE Trans. Circuits Syst* **35** (10) (1988) 1257–1272.

[11] L. O. Chua, Chua's Circuit: Ten years later. *IEICE Trans. Fundamentals* **E77** A(11) (1994) 1811–1822.

[12] L. Pecora and T. Carroll, Synchronization in chaotic systems, *Physical Review Letters* **64** (1990) 821–824.

[13] M. Yalcin, J. Suykens, and J. Vandewalle, *Cellular Neural Networks, Multi-Scroll Chaos and Sychronization*, World Scientific Publishing, 2005.

[14] P. Arena S. Baglio, L.fortuna, and G.Manganaro, Chua's circuit can be generated by CNN cell, *IEEE Trans. Circuit and Systems –I* **42** (2) (1995) 123–125.

[15] P. S. Swathy, K. Thamilmaran, An experimental study on SC-CNN based canonical Chua's circuit, *Nonlinear Dyn* **71** (2013) 505–514.

[16] R. Rhouma, S. Meherzi, S. Belghith, OCML-based colour image encryption, *Chaos, Solitons Fractals* **40** (1) (2008) 309–318.

[17] S. Pakiriswamy and S. Vaidyanathan, The active controler design for achieving generalized projective synchronization of hypechaotic Lu and hyperchaotic Cai system, *IJAIT*, **2** (2012) 75–92.

[18] Chen G, Mao Y, Chui C. A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos, Solitons Fractals* **21** (3) (2004) 749–761.

Ngày nhận bài 11 - 6 - 2013

Nhận lại sau sửa ngày 27 - 8 - 2013