

MỘT PHƯƠNG PHÁP MÃ HÓA ẢNH DỰA TRÊN TÍNH TOÁN DNA VÀ HỆ HỖN LOẠN LORENZ

Nguyễn Văn Căn*, Đoàn Ngọc Tú

Tóm tắt: Bài báo này, chúng tôi đề xuất một mô hình mã hóa ảnh sử dụng mã hóa DNA trên hệ hỗn loạn Lorenz. Bao gồm 6 giai đoạn: đầu tiên ảnh gốc được nhập vào; tiền xử lý nhị phân và biến đổi DNA; biến đổi trên hệ hỗn loạn; xử lý các tính toán di truyền (định hình, lai ghép, đột biến); mã hóa với khóa bí mật; thu được ảnh mã hóa. Điểm nổi bật của mô hình là sử dụng kết hợp luật di truyền của DNA và hệ hỗn loạn Lorenz để tiến hành mã hóa. Việc kiểm tra sự hiệu quả của mô hình được kiểm nghiệm bằng các kiểm tra các thông số như lược đồ xám, sự tương quan, và so sánh mô hình với phương pháp mã hóa ADN thông thường.

Từ khóa: DNA Encryption; Chaotic; Lorenz; Image Encryption.

1. MỞ ĐẦU

Ảnh số là thông tin quan trọng của truyền thông đa phương tiện, vấn đề bảo mật ảnh trở thành một vấn đề quan tâm chung cho mọi người. Mã hóa ảnh là sử dụng các phương pháp mã hóa để thay đổi ảnh từ định dạng bình thường sang dạng được che giấu, nếu không có quyền truy xuất và khóa giải mã thì không xem được. Hiện nay đã có rất nhiều thuật toán được phát triển cho mục đích này. Như sử dụng mẫu G-Scant[1], hệ hỗn loạn Lorenz[5], tính toán ADN([1], [2], [6], [8], [9]). Tuy nhiên, một số phương pháp lại gặp phải một số hạn chế nhất định.

Trong bài báo này, chúng tôi đề xuất mô hình sử dụng kỹ thuật di truyền trong DNA kết hợp trên hệ hỗn loạn Lorenz để mã hóa ảnh. Ảnh đầu vào được chuyển về cấu trúc của DNA, định hình lại cấu trúc và sử dụng các phương pháp lai ghép, đột biến để biến đổi cấu trúc của đoạn mã DNA. Định hình lại trên hệ hỗn loạn Lorenz. Số lần lai ghép, đột biến, khóa giải mã, các tham số đầu vào của hệ hỗn loạn Lorenz sẽ được người gửi và người nhận sử dụng chung để giải mã các thông tin có trong hình ảnh được mã hóa. Các kỹ thuật này được áp dụng nhằm tăng tính bảo mật trên ảnh được mã hóa, tăng độ nhiễu, hạn chế việc sử dụng các phương pháp vét cạn để đoán khóa giải mã. Kết quả thực nghiệm so sánh với mô hình mã hóa DNA thông thường cho thấy kỹ thuật sử dụng phương pháp mã hóa DNA trên hệ hỗn loạn Lorenz có mức độ bảo mật cao và tốt hơn.

Phần tiếp theo (phần 2) giới thiệu về mã hóa DNA và một số tính chất, phần 3 giới thiệu về hệ hỗn loạn Lorenz, phần 4 trình bày mô hình đề xuất của chúng tôi, phần cuối là các kết quả thử nghiệm và đưa ra kết luận.

2. MÃ HÓA DNA

DNA (DeoxyriboNucleic Acid) là một vật chất di chuyển, được tìm ra vào năm 1969 bởi Miescher. Trong DNA có 4 giá trị được biểu diễn là: A (adenine), C (cytosine), G (guanine), T (thymine) [6][9]. Ta có thể sử dụng các giá trị của DNA làm đại diện cho các bit trong biểu diễn ảnh, với A, C, G, T trong DNA tương ứng với 00, 01, 10, 11 trong nhị phân. Lợi ích khi sử dụng mã hóa DNA như: mật độ thông tin bất thường; cung cấp mức độ tính toán song song lớn; tiêu thụ tài nguyên cực thấp[1]. Sau khi biến đổi các bit về chuỗi DNA, ta có thể sử dụng một số phương pháp di truyền để biến đổi, định hình lại chuỗi nhằm tạo ra đầu ra được mã hóa theo quy luật nhất định.

2.1. Định hình

Một chuỗi DNA sẽ được định hình thành các phân đoạn có kích thước bằng nhau, nhằm tạo ra các quy định về cấu trúc thống nhất cho các giai đoạn di truyền tiếp theo.

Trong các giai đoạn định hình này, các điểm đầu và chiều dài của các đoạn DNA sẽ được xác định. Sau mỗi vòng lặp, các tham số này có thể được giữ nguyên hoặc được thay đổi.

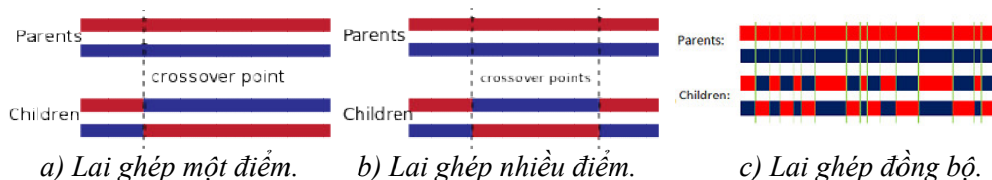
2.2. Lai ghép

Lai ghép là một trong những tính chất di truyền ứng dụng được trong mã hóa DNA. Với hai mẫu cha mẹ, sau quá trình lai ghép, các mẫu con sẽ thừa hưởng một số đặc tính của cả cha và mẹ. Có ba dạng lai ghép phổ biến:

- Lai ghép 1 điểm sử dụng một điểm nút, sau đó các đoạn mã DNA của các mẫu cha mẹ sẽ được chuyển cho nhau, tạo ra các mẫu con chứa một đoạn thông tin của cha và một đoạn thông tin của mẹ.

- Lai ghép nhiều điểm sử dụng 2 hoặc nhiều điểm nút, lần lượt các đoạn mã DNA có thứ tự chẵn nằm giữa 2 điểm nút của cha và mẹ liên tiếp sẽ được chuyển cho nhau, tạo ra các mẫu con lai nhiều đoạn thông tin của cha và mẹ.

- Lai ghép đồng bộ và nửa đồng bộ là lai nhiều đoạn của cha và mẹ, các điểm nút được sinh ngẫu nhiên, sao cho các mẫu con chứa 50% mã DNA của cha và 50% mã DNA của mẹ.



Hình 1. Các dạng lai ghép.

2.3. Đột biến

Đột biến là quá trình thay đổi các giá trị của các phần tử trong chuỗi. Bao gồm: Biến đổi trong bit là phương pháp truyền thông cổ điển được sử dụng trong các dây bit, trong một đoạn bit m và n bất kỳ, các đoạn bit 0 sẽ được chuyển sang bit 1 và ngược lại; Biến đổi trong chuỗi DNA là phương pháp đột biến trên DNA, tương tự như biến đổi trong bit, ta có thể sử dụng đột biến trong 1 khoảng bất kỳ, hoặc toàn bộ chuỗi DNA, Quy luật biến đổi như sau giá trị $A \rightarrow T$; $T \rightarrow A$; $G \rightarrow C$; $C \rightarrow G$.

3. HỆ HỖN LOẠN

Hệ hỗn loạn là hệ mà khi có thay đổi nhỏ các tham số đầu vào dẫn tới sự khác biệt rất lớn trong các hành vi thực hiện của hệ đó. Hỗn loạn là một hành vi không xác định, ngẫu nhiên, không có chu kỳ, tính hội tụ và tính gom nhóm. Hệ hỗn loạn có tính thất thường, được tạo thành từ một quá trình tiền định (từ hệ phương trình vi phân thường). Quỹ đạo nghiệm phương trình vi phân thường rất nhạy cảm với giá trị đầu. Hệ hỗn loạn hiện đang có nhiều ứng dụng trong bảo mật thông tin ([5], 10)). Một số hệ hỗn loạn phổ biến như hệ Lorenz, Logistic,...

3.1. Hệ hỗn loạn Lorenz

Năm 1963, Edward Lorenz, nhà khí tượng học, đã phát triển một mô hình đối lưu đơn giản trong khí quyển. Bằng cách giữ hầu hết các biến số liên tục, đã giảm hệ thống xuống không gian trạng thái ba chiều[3]. Hệ Lorenz có mô hình tiền định ba chiều [4]:

$$\begin{cases} x' = \sigma(y - x) \\ y' = x(\rho - z) - y \\ z' = xy - \beta z \end{cases} \quad (1)$$

trong đó, $\underline{p} = (\sigma, \rho, \beta)^T$ với σ, ρ, β là các số thực dương, là vector các tham số mô hình và $\underline{x} = (x, y, z)^T$ là quỹ đạo của hệ. Quỹ đạo nghiệm $x(t, x_0, p)$ của hệ Lorenz luôn bị chặn với mọi giá trị đầu x_0 .

3.2. Ứng dụng của hệ hỗn loạn Lorenz trong mã hóa bảo mật

Để mã hóa một ký tự m trong thông tin M nhờ phân tử $x_i(t, x_0, p)$ của quỹ đạo $x(t, x_0, p)$ thì $x_i(t, x_0, p)$ sẽ được trích mẫu thành N giá trị.

$$m_j = x_i(t, x_0, p), j = 1, 2, 3, \dots, N \quad (2)$$

trong đó T là chu kỳ trích mẫu và N là giá trị được chọn đủ lớn. Tiếp tục, xác định: 2 điểm a và b với $a > b$. Chia khoảng cách giữa a và b thành t khoảng đều nhau (t là số lượng điểm ảnh có trong ảnh cần mã hóa).

$$\varepsilon = \frac{a-b}{t} \quad (3)$$

Xây dựng thông tin M' mới được sắp xếp lại các giá trị của M theo chiều tăng dần, hoặc giảm dần. Khi đó, giá trị $a + \varepsilon$, được lưu trong M sẽ có vị trí tương ứng mới trong M' . Lúc này ta có bảng M và M' là bảng mã hóa và giải mã của ảnh. Các điểm ảnh lưu trong bức ảnh ở vị trí số đầu tiên trong M sẽ có vị trí mới tương ứng chỉ số của nó được lưu trong mảng M' .

4. MÔ HÌNH MÃ HÓA ẢNH BẰNG MÃ HÓA DNA VÀ HỆ HỖN LOẠN

Trong mô hình này, chúng tôi đề xuất việc sử dụng mã hóa DNA và biến đổi các vị trí của ảnh được biểu diễn dưới dạng DNA trên hệ hỗn loạn. Sau đó tiếp tục tiến hành các biến đổi di truyền trên các đoạn DNA và cuối cùng mã hóa kết quả với khóa để tạo ra ảnh mã hóa. Các giai đoạn của mô hình được mô tả như sau:

4.1. Giai đoạn tiền xử lý

Bước tiền xử lý có thể tổng quan như sau: Bất kỳ tập dữ liệu nào cũng có thể được biểu diễn dưới dạng nhị phân (văn bản, hình ảnh, video, dữ liệu). Các dữ liệu này được phân chia thành các nhóm 8bit, mỗi bit liền kề được chuyển thành 4 giá trị cơ sở của DNA: A, C, G, T. Ví dụ: 10 11 01 00 10 11 10 11 00 10 01 01 11 01
Chuyển đổi từ dạng nhị phân trên thành dạng DNA: GTCAGTGTAGCCTC.

4.2. Mã hóa bằng DNA

Trước tiên là sinh khóa cho chuỗi DNA. Khóa có thể là một chuỗi DNA hoặc là dạng nhị phân. Ở đây sử dụng khóa chính là hàm băm SHA256 của chuỗi DNA sau khi biến đổi. Tiến hành XOR khóa với dữ liệu trước hoặc sau khi biến đổi. Có 2 phương pháp mã hóa với khóa là XOR với bit nhị phân, hoặc XOR với giá trị DNA. Đối với phép XOR sử dụng DNA, ta sử dụng bảng mã hóa sau:

Bảng 1. Quy tắc XOR của DNA.

XOR	A	G	C	T
A	A	G	C	T
G	G	A	T	C
C	C	T	A	G
T	T	C	G	A

Ví dụ: Ta có bản rõ nhị phân: 10 11 01 00 10 11 10 11 00 10 01 01 11 01, khóa bí mật là: "khoa": 01 10 10 11 01 10 10 00 01 10 11 11 01 10 00 01, XOR khóa bí mật với bản rõ, ta có bản mã như sau:

11 00 00 00 01 00 01 11 10 11 10 10 01 11 100.

Đối với bản rõ là DNA ta xét ví dụ bản rõ GTCAGTGTAGCCTC, khóa bí mật "khoa" được chọn dạng DNA là: CGGTCCGACGTTTCGAC, tiến hành XOR khóa bí mật với bản rõ được: ACTTTCACATTAA.

4.3. Biến đổi theo các tính chất di truyền

Sau khi mã hóa, ta đã có được bản mã lưu trữ dưới dạng DNA. Sau đó áp dụng các quy định di truyền để thực hiện việc lai ghép, đột biến sau một số lần lặp xác định.

Bảng 2. Một số tính chất trong mỗi vòng lặp.

STT	Các bước thực hiện mỗi vòng lặp
1	Đột biến → Lai ghép
2	Lai ghép → Đột biến
3	Lai ghép → Đột biến → Lai ghép
4	Đột biến → Lai ghép → Đột biến

Với các vòng lặp lẻ có thể xây dựng quy trình khác so với các vòng lặp chẵn để đảm bảo các dữ liệu được trộn đúng quy luật nhằm đảm bảo tính thống nhất trong chu trình mã hóa và giải mã.

4.4. Biến đổi trên hệ hỗn loạn Lorenz

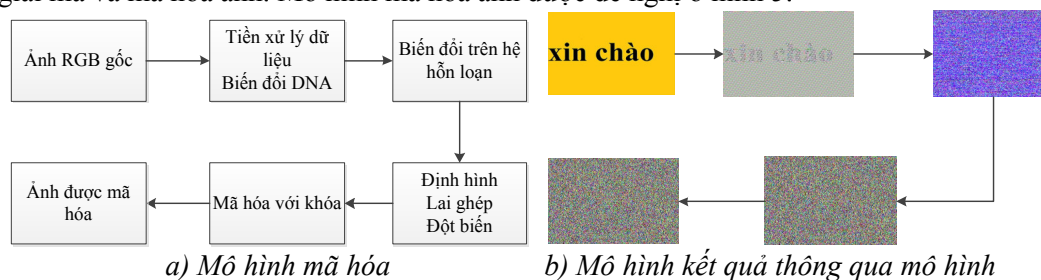
Thực hiện xây dựng bảng mã trên hệ hỗn loạn Lorenz theo công thức (1). Các bước xây dựng:

Input: Kích thước ảnh m,n , các tham số σ, ρ, β

Output: Bảng mã C xây dựng trên các tham số đã cho

- Mảng A $\leftarrow m*n*4$
- Xây dựng bảng rõ dựa trên các giá trị của mảng A theo (1)
- Xây dựng bảng mã bằng phương pháp sắp xếp
 $B \leftarrow \text{sort}(A)$
- Xây dựng bảng mã hóa dựa trên 2 mảng A và B
 $C \leftarrow \text{bsearch}(A,B)$ (Mảng C lưu các vị trí các phần tử của A trong mảng B)

Mảng C lưu các vị trí mới trong bức ảnh, chính là mảng được sử dụng phục vụ việc giải mã và mã hóa ảnh. Mô hình mã hóa ảnh được đề nghị ở hình 5.



Hình 2. Mô hình mã hóa ảnh và dạng kết quả.

Mô hình đề nghị được mô tả bằng thuật toán:

THUẬT TOÁN MÃ HÓA	THUẬT TOÁN GIẢI MÃ
Input: Dữ liệu ảnh gốc Output: Ảnh được mã hóa	Input: Dữ liệu ảnh được mã hóa Output: Ảnh được giải mã
<ol style="list-style-type: none"> BData \leftarrow Mã nhị phân của ảnh gốc Định hình Bdata Nhóm 2 bit nhị phân liền kề DNADData \leftarrow BData While (Vòng lặp n \neq 0) do Định hình DNADData DNADData' \leftarrow Lai ghép các phân đoạn DNADData' DNADData'' \leftarrow Đột biến trên DNADData' DNADData \leftarrow DNADData'' End while Mã hóa DNADData trên hệ hỗn loạn Lorenz 	<ol style="list-style-type: none"> BData \leftarrow Mã nhị phân của ảnh mã hóa Định hình Bdata Nhóm 2 bit nhị phân liền kề DNADData \leftarrow BData Xor DNADData với khóa K. Giải mã DNADData trên hệ hỗn loạn Lorenz While (Vòng lặp n \neq 0) do Định hình DNADData DNADData'' \leftarrow Đột biến trên DNADData' DNADData' \leftarrow Lai ghép các phân đoạn DNADData'

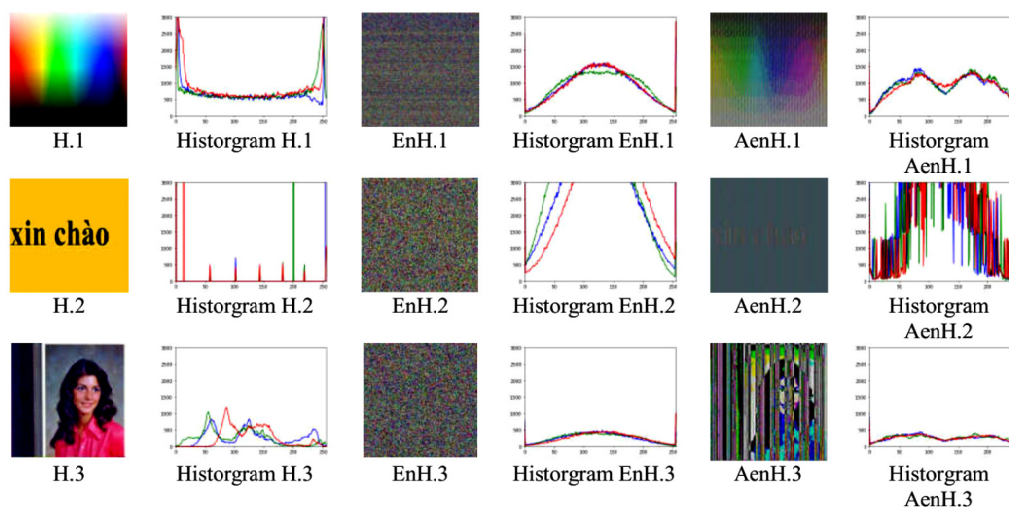
12. Xor DNADData với khóa K.	11. DNADData ← DNADData''
13. Định hình DNADData	12. End while
14. BData ← DNADData	13. Định hình DNADData
15. Ảnh mã hóa ← BData	14. BData ← DNADData
	15. Ảnh giải mã ← BData
	16. if (SHA256(Ảnh giải mã) = key)
	17. then end else giải mã không thành công

5. KIỂM THỬ VÀ ĐÁNH GIÁ AN TOÀN

5.1. Môi trường và dữ liệu thực nghiệm

Mô hình được thử nghiệm trên ngôn ngữ lập trình Python 3, sử dụng máy tính có CPU Core i7-3740 2.70Hz, Ram 8Gb và sử dụng hệ điều hành windows 7 Professional 64 bits. Kiểm tra một số phương pháp thám mã như phân tích không gian, độ nhạy của khóa; phân tích lược đồ xám; tỉ lệ điểm ảnh thay đổi và phân tích hệ số tương quan giữa các điểm ảnh lân cận trong ảnh gốc và ảnh mã hóa. Thử nghiệm với 3 loại: ảnh màu có dải màu rộng, ảnh màu RGB đơn điệu và ảnh màu RGB nhiều chi tiết; đối sánh các kết quả với phương pháp mã hóa ADN thông thường. Các ảnh sau khi được mã hóa bằng mô hình đề xuất được kí hiệu là EnH.1, EnH.2, EnH.3; bằng mã hóa ADN được ký hiệu là AenH.1, AenH.2, AenH.3. Bộ tham số sử dụng trên hệ hỗn loạn Lorenz như sau: $\sigma = 10$, $\rho = 28$, $\beta = 2.667$.

5.2. Phân tích lược đồ xám



Hình 3. Lược đồ xám của ảnh gốc và ảnh mã hóa.

Một hình ảnh màu mã hóa được coi là lý tưởng nếu như có phân bố đồng đều dải màu. Hình trên đã minh họa các lược đồ xám của ảnh gốc và ảnh mã hóa. Từ các ảnh gốc ban đầu có các lược đồ xám khác nhau, sau khi mã hóa đều thu được các ảnh có độ nhiễu và lược đồ xám gần tương tự nhau. Mô hình đề xuất có biểu đồ histogram đồng đều hơn so với chỉ sử dụng mã hóa ADN. Điều đó cho thấy không thể khai thác các thông tin lược đồ xám trên ảnh được mã hóa để thám mã ảnh.

5.3. Phân tích các hệ số tương quan

Một phương pháp để đánh giá chất lượng mã hóa của một phương pháp mã hóa hình ảnh là đánh giá các hệ số tương quan giữa các điểm ảnh liền kề trong ảnh gốc và ảnh được mã hóa. Theo [1] ta có:

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (4)$$

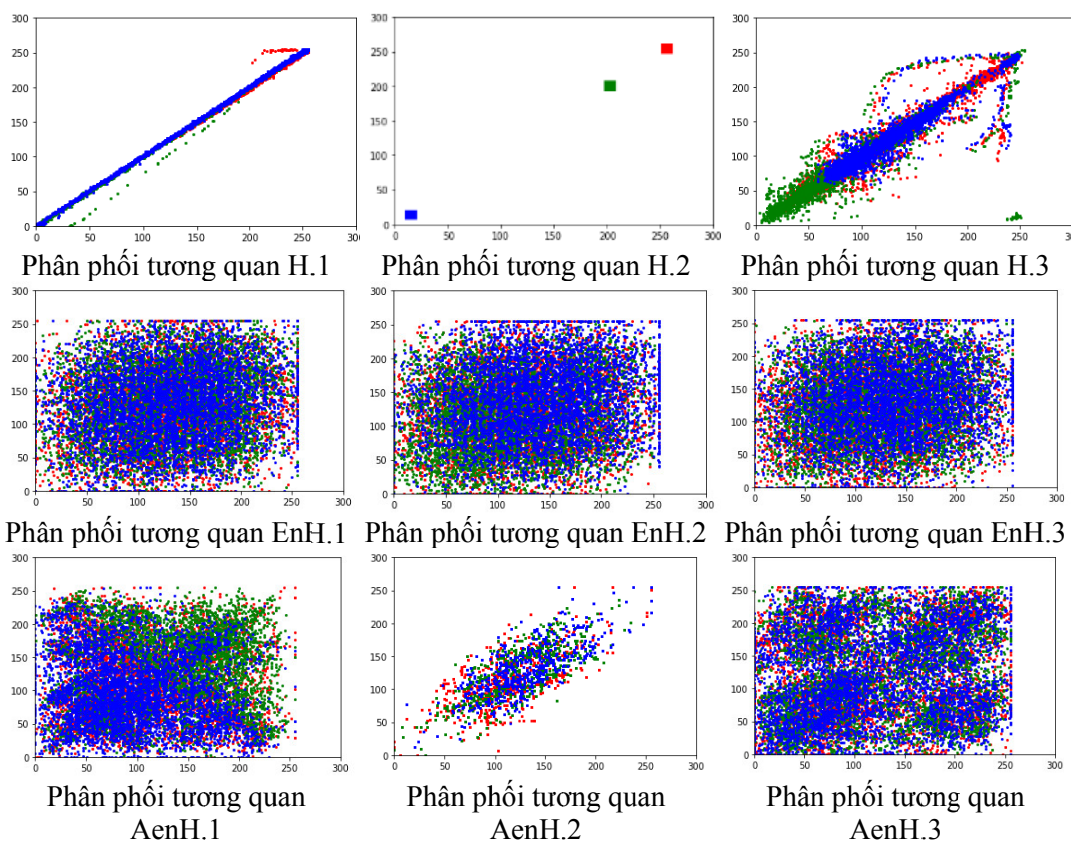
Với, x và y là các giá trị của 2 điểm ảnh liên kế nhau.

$$E(x) = \frac{1}{L} \sum_{l=1}^L x_l \quad (5)$$

$$D(x) = \frac{1}{L} \sum_{l=1}^L (x_l - E(x))^2 \quad (6)$$

$$cov(x,y) = \frac{1}{L} \sum_{l=1}^L (x_l - E(x)) - (y_l - E(y)) \quad (7)$$

Trong đó, L là số lượng điểm ảnh. Khi r càng nhỏ, thuật toán càng hiệu quả [1]. Thực nghiệm với 5000 điểm ảnh được trích xuất ngẫu nhiên từ ảnh gốc và ảnh mã hóa trong dữ liệu kiểm thử, lược đồ phân phối tương quan (hình 5) và bảng hệ số tương quan giữa các điểm ảnh láng giềng (bảng 3).

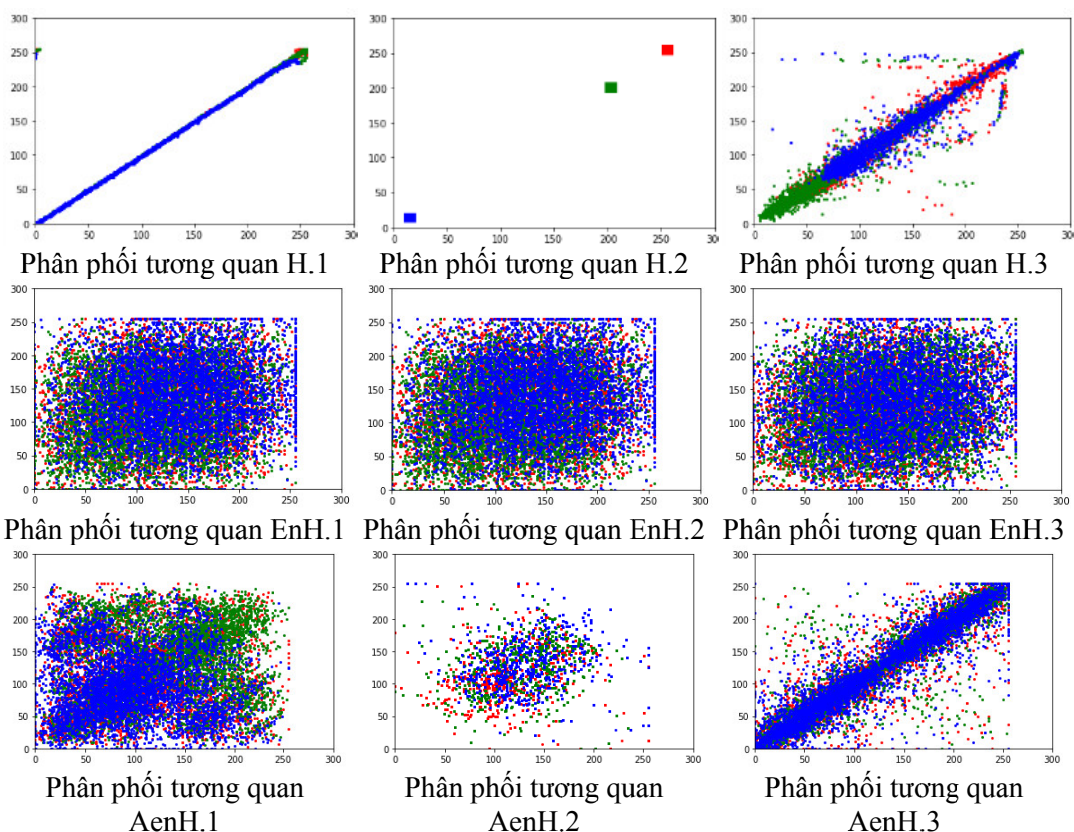


Hình 4. Lược đồ phân phối tương quan của 2 điểm ảnh liên kế theo chiều dọc trong ảnh gốc và ảnh được mã hóa.

Bảng 3. Hệ số tương quan trong các điểm ảnh giữa ảnh gốc và ảnh mã hóa đối với thuật toán đề xuất.

		Hình 1			Hình 2			Hình 3		
		H.1	EnH.1	AenH.1	H.1	EnH.2	AenH.2	H.1	EnH.3	AenH.3
Chiều dọc	Red	0.7197	0.0963	0.0951	nan	0.1382	0.2427	0.981	0.1348	0.9286
	Green	0.9596	0.1509	0.1595	nan	0.1519	0.2471	0.9752	0.1495	0.9355

	Blue	0.9724	0.0875	0.0572	nan	0.1406	0.1652	0.9544	0.1492	0.9256
Chiều ngang	Red	0.995	0.1516	0.0044	nan	0.1183	0.6833	0.9653	0.1422	0.1808
	Green	0.9999	0.162	0.0618	nan	0.1359	0.7467	0.9311	0.1265	0.1922
	Blue	0.9997	0.1008	0.1174	nan	0.1343	0.7564	0.9418	0.1671	0.186
Đường chéo	Red	0.7497	0.0394	0.6476	nan	0.0744	nan	0.9498	0.0909	0.9496
	Green	0.966	0.0738	0.9573	nan	0.0788	nan	0.9063	0.0658	0.9055
	Blue	0.9763	0.0235	0.9415	nan	0.0763	nan	0.902	0.0749	0.9065



Hình 5. Lược đồ phân phối tương quan của 2 điểm ảnh liên kề theo chiều ngang trong ảnh gốc và ảnh được mã hóa.

Qua các lược đồ, ta có thể thấy đối với lược đồ phân phối tương quan, các lược đồ của mô hình đề xuất đạt ở mức ổn định, các điểm ảnh phân phối đều theo 2 chiều. Còn đối với ảnh mã hóa bằng DNA, các lược đồ không ổn định. Một số lược đồ còn có tỉ lệ tương đồng cao so với ảnh gốc.

5.4. Tỉ lệ số lượng điểm ảnh thay đổi

NPCR (Number of Pixels Change Rate) [1] là tỉ lệ số điểm ảnh thay đổi trong ảnh gốc so với ảnh mã hóa. Tỉ lệ NPCR càng cao (càng gần 100) thì sự thay đổi trong ảnh gốc càng lớn. Tỉ lệ này tỉ lệ thuận với hiệu quả cho việc chống lại các tấn công known-plaintext attack. Tỉ lệ NPCR được tính như sau:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M.N} \cdot 100\% \quad (8)$$

Tính toán NPCR trên tập ảnh thử nghiệm có kết quả:

Bảng 4. Tỷ lệ NPCR giữa ảnh gốc và ảnh mã hóa.

NPCR	H.1 - EnH.1	H.2 - EnH.2	H.3 - EnH.3	H.1 - AenH.1	H.2 - AenH.1	H.3 - AenH.1
Red	99.198024	98.851314	98.78845	99.32517	99.06606	98.744201
Green	99.274055	99.422605	98.77930	99.39991	99.018372	98.767089
Blue	99.235395	99.655096	98.69995	99.28006	99.39294	98.730468

Bảng 4 cho thấy, tỉ lệ điểm ảnh thay đổi giữa các ảnh của mô hình đề xuất và mã hóa DNA đều đạt ở mức cao, tất cả đều trên 98,5%. Điều đó chứng tỏ mô hình thuật toán đạt hiệu quả cao trong việc chống lại tấn công known-plaintext attack trên ảnh mã hóa. Kết hợp với hệ số tương quan, ta có thể kết luận, mô hình đề xuất đảm bảo các tỉ lệ điểm ảnh thay đổi và giảm được các hệ số tương quan giữa các điểm ảnh theo các chiều ngang, dọc và chéo. Đảm bảo các nguyên tắc mã hóa ảnh, biến đổi ảnh mã hóa tốt hơn so với mã hóa bằng DNA thông thường.

6. KẾT LUẬN

Trong bài báo này, chúng tôi đã đề xuất một mô hình mã hóa, cải tiến sử dụng mã hóa DNA trên hệ hỗn loạn Lorenz. Trong đó, sử dụng một số luật di truyền của DNA để tiến hành biến đổi, mã hóa theo quy luật sau đó sử dụng hệ hỗn loạn Lorenz để tạo ra một bức ảnh có nội dung hỗn loạn, ngẫu nhiên. Bài báo cũng đã phân tích một số đặc điểm an toàn trên bức ảnh được mã hóa, qua các chỉ số và lược đồ đánh giá, có thể thấy mô hình có chất lượng ảnh mã hóa tốt hơn so với mã hóa bằng DNA. Tuy nhiên, mô hình trong còn một số vấn đề còn tồn tại như cải tiến về độ mã hóa, tăng độ nhiễu trong bức ảnh cũng cần được phải nghiên cứu trong tương lai.

TÀI LIỆU THAM KHẢO

- [1]. Aarti Patel, Dr.Mehul Parikh, "A Survey on Multiple Image Encryption Using Chaos Based algorithms And DNA Computing". NCARTICT-2018.
- [2]. M. Mitchell, "An Introduction to Genetic Algorithms", MIT Press, 1998.
- [3]. M. Mousa, "DNA-Genetic Encryption Technique", Computer Network and Information Security, vol 7, pp. 1-9, 2016.
- [4]. H. Khodadadi, O. Mirzaei, "A stack-based chaotic algorithm for encryption of colored images", Journal of AI and Data Mining, vol 5, pp. 29-37, 2017.
- [5]. Jinhua Lu, "A new chaotic system and beyond: the generalized lorenz-like system", International Journal of Bifurcation and Chaos, vol 14, no 5, pp. 1570 - 1537, 2004.
- [6]. C. T. Celland, V. Risca and Bancroft C, "Hiding messages in DNA microdots", Nature, vol. 399, pp. 533-534, 1999.
- [7]. Leier, A., Richter, C., Banzhaf, W. and Rauhe, H. "Cryptography with DNA Binary Strands", BioSystems, Vol. 57, pp.13-22, 2000.
- [8]. Mohammadreza, Najaforkaman, Nazanin Sadat Kazazi, "A Method to Encrypt Information with DNA-Based Cryptography", International Journal of Cyber-Security and Digital Forensics (IJCSDF) 4(3): pp. 417-426, 201.
- [9]. Qiang Zhang, Xiaopeng WeiRGB, "Color Image Encryption Method Based on Lorenz Chaotic System and DNA Computation", Journal IETE Technical Review, pp.404-409, 2014.

ABSTRACT

A MODEL OF IMAGE ENCODING USING DNA AND LORENZ CHAOS

In this paper, we propose an image coding model using DNA encoding on Lorenz chaos. It consists of 6 stages: first the original image is entered; binary processing and DNA modification; transformation on chaos; processing of genetic calculations (shaping, hybridization, mutation); Encrypt with secret key; obtained image encoded. The highlight of the model is the use of combining the genetic laws of DNA and the Lorenz chaos system to conduct coding. Testing of model performance was tested by testing parameters such as histogram, correlation, etc...

Keywords: DNA Encryption; Chaotic; Lorenz; Image Encryption.

Nhận bài ngày 01 tháng 7 năm 2018

Hoàn thiện ngày 10 tháng 9 năm 2018

Chấp nhận đăng ngày 20 tháng 9 năm 2018

Địa chỉ: Trường Đại học Kỹ thuật - Hậu cần CAND.

* Email: cannv@truongt36.edu.vn.